Rational points on elliptic curve & computation of rank of elliptic curve

Pradeep Kumar Mishra

A Thesis Submitted to

Indian Institute of Technology Hyderabad

In Partial Fulfillment of the Requirements for

The Degree of Master of science

भारतीय प्रौद्योगिकी संस्थान हैदराबाद

Indian Institute of Technology Hyderabad

Department of mathematics

May 2015

DECLARATION

I declare that this written submission represents my ideas in my own words and where others' ideas or words 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 any idea in my submission. I understand that any violation of the above will be cause for disciplinary action by the Institute and can also evoke penal action from the source which have thus not been properly cited or from whom proper permission has not been taken when needed.

CH.V.G.N.Kumar

(Signature of the supervisor)

CH V G Narasimha Kumar

(Name of the supervisor)

Pradeep Mishra.

(Signature of the student)

Pradeep Kumar Mishra

(Name of the student)

MA13M1006

(Roll no)

Date: 19/06/15

Place: Hyderabad

APPROVAL SHEET

This thesis entitled "RATIONAL POINTS ON ELLIPTIC CURVE & COMPUTAION OF RANK OF ELLIPTIC CURVE" by PRADEEP KUMAR MISHRA is approved for the degree of MASTER OF SCIENCE.

CH.V.G.N.Kumar

(Signature of the supervisor)

CH VG Narasimha Kumar.

(Name of the supervisor)

Date: 19/06/2015

Place: Hyderabad.

Acknowledgements

I would like to express my high regard to my guide Dr. Narasimha for his unflinching support constant visit while I set about the project. I am ever so thankful to you sir for your co-operation suggestions without which this project would not have seen the light of day.

Pradeep Kumar Mishra.

Dedication

I dedicate my dissertation work to my family and many friends. A special feeling of gratitude to my loving parents whose words of encouragement and push for tenacity ring in my ears. My brothers Sandeep Kumar Mishra has never left my side and are very special.

Contents

List of Notation

E	Elliptic curve
$\mathbb{N}$	Set of natural numbers
$\mathbb{Z}$	Set of integers
$\mathbb{Q}$	Set of rational numbers
$\mathbb{R}$	Set of real numbers
$\mathbb{C}$	Set of complex numbers.
C	Cubic curve
K	Field
$\bar{K}$	Algebraic closed field
$\mathbb{A}^n(K)$	n- dimensional affine space
$\mathbb{P}^2_K$	Projective plane over field K
$P * Q$	Composition law on elliptic curve for ponits P and Q
$P + Q$	Addition law on elliptic curve
$\mathcal{O}$	Point at infinity on a cubic curve
$E(\mathbb{Q})$	Set of all rational points on E
$E(\mathbb{R})$	Set of all real points on E
$E(\mathbb{C})$	Set of all complex points on E
$\triangle$	Discriminant of a polynomial
E_λ	Legendre form of elliptic curve
$\mathbb{Z}[x]$	Polynomial with integer coefficients
$\mathbb{Z}/n\mathbb{Z}$	Intgers modulo n
$E(p^v)$	Rational points with p^v in denominator
$H(x)$	Height of a rational number x
$H(P)$	Height of a point $P = (x, y)$ on a cubic curve
$h(P)$	logarithm of $H(P)$
ord	Order of a rational number

Chapter 1

Geometry and Arithmetic

In this chapter we will introduce some definitions and facts which will be useful. We will see how to get rational points on elliptic curve. We will give the composition law on the set of rational points on elliptic curve by this composition law and we will show that $E(\mathbb{Q})$ is a group. Moreover it is Abelian.

1.1 Algebraic Geometry

In this section we will discuss some definitions like affine space, affine variety, projective space etc which we will use .

Definition 1.1.1. *Given a field K and a positive integer n, we define the n-**dimensional affine space** $\mathbb{A}^n$ over k to be the set*

$$\mathbb{A}^n(K) = \{(a_1, \ldots, a_n) : a_1, \ldots, a_n \in K\}$$

Definition 1.1.2. *Let K be a field, and let $f_1, f_2, \ldots, f_s$ be polynomials in $K[x_1, \ldots, x_n]$. Then we set*

$$V(f_1, f_2, \ldots, f_s) = \{(a_1, a_2, \ldots, a_n) \in K^n : f_i(a_1, \ldots, a_n) = 0\} \qquad \forall\ 1 \leq i \leq s$$

*We call $V(f_1, f_2, \ldots, f_s)$ the **affine variety** defined by $f_1, f_2, \ldots, f_s$. Thus, an affine variety $V(f_1, \ldots, f_s) \subset K^n$ is the set of all solutions of the system of equations $f_1(x_1, \ldots, x_n) = \cdots = f_s(x_1, \ldots, x_n) = 0$.*

We begin in the plane $\mathbb{R}^2$ with the variety $V(x^2 + y^2 - 1)$, which is the circle of radius 1 centered at the origin given by the following figure 1.1. An interesting example of a curve in $\mathbb{R}^3$ is the twisted cubic,

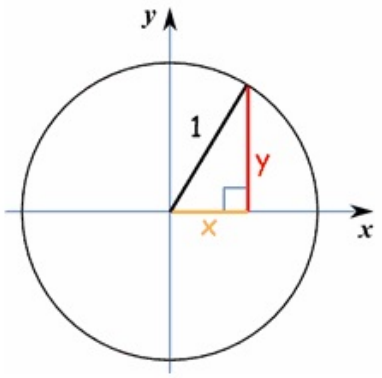


Figure 1.1:

which is the variety $V(y - x^2, z - x^3)$. For simplicity, we will confine ourselves to the portion that lies in

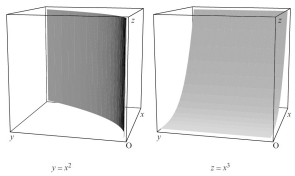


Figure 1.2:

the first octant. To begin, we draw the surfaces $y = x^2$ and $z = x^3$ separately given by the following figure 1.2. Then their intersection gives the twisted cubic given by the following figure 1.3.

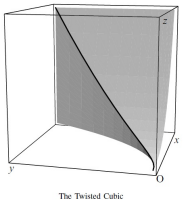


Figure 1.3:

Definition 1.1.3. *The **projective plane** is defined as the set of all triples (a, b, c), such that a, b and c are not all 0, and where (a, b, c) is considered to be the same point as (a', b', c') if $(a', b', c') = (ta, tb, tc)$ for some nonzero t.*

In other words, the projective plane is defined in terms of an equivalence relation $\sim$ on all triples of homogeneous coordinates (a, b, c), such that $(a, b, c) \sim (a', b', c')$ if and only if $a' = ta, b' = tb, c' = tc$ for some nonzero t. This equivalence relation allows for the following simplified definition of $\mathbb{P}^2_K$:

$$\mathbb{P}^2_K = \frac{\{(a, b, c) |\ a, b, c \in K \text{ are not all } 0\}}{\sim}$$

This definition lends itself to a somewhat more intuitive definition of the projective plane. If a triple (a, b, c) is to be thought of as a vector in $\mathbb{R}^3$, then the vector (a, b, c) is considered equivalent to all scalar multiples of the vector itself. Thus, for any given triple (a, b, c) the set of all triples considered equivalent to (a, b, c) is the line passing through the origin and (a, b, c). Because all points in a given direction from the origin are equivalent in projective space, the projective plane can simply be thought of as including the set of all directions in $\mathbb{R}^3$.

An interesting implication is the notion of point at infinity. Because any two parallel lines in $\mathbb{A}^2$ must by definition have the same direction, in projective space the lines must have the point defining their direction in common. This intersection is the basis for the notion of a “point at infinityâĂİ -it is the point at which two parallel lines traveling in a given direction must intersect in projective space. In order to maintain the property that two lines may only intersect at one point, there must be a point at infinity for every given direction in Thus, projective space can also be defined as :

$$\mathbb{P}^2 = \mathbb{A}^2 \cup \{ \text{ The set of directions in } \mathbb{A}^2 \}$$

It is important to remember that both projective space and affine space are defined over a field.

Definition 1.1.4. *A **cubic curve** in projective space is defined as the set of solutions of a polynomial function $F(X, Y, Z)$ such that*

$$E : F(X, Y, Z) = 0$$

More specifically, because such curves exist in projective space, the polynomial $F(X,Y,Z)$ must be homogeneous of degree d. This means that it must satisfy the property :

$$F(tX,tY,tZ) = t^d F(X,Y,Z),$$

where d is the degree of the polynomial F.

Definition 1.1.5. *Let $F(X,Y,Z) = 0$ is an projective plane and let (X_0,Y_0,Z_0) be any point on the curve such that*

$$\left(\frac{\partial F}{\partial X}(X_0,Y_0,Z_0), \frac{\partial F}{\partial Y}(X_0,Y_0,Z_0), \frac{\partial F}{\partial Z}(X_0,Y_0,Z_0)\right) \neq (0,0,0)$$

*Such a point is called a **non-singular** point on the curve . If every point on the curve is non singular then then we say our curve is non singular. A point which is not non-singular is called a **singular** point.*

Definition 1.1.6. *Let $f(x,y) = 0$ is an affine plane and let (x_0,y_0) be any point on the curve such that the partial derivatives do not both vanish,*

$$\left(\frac{\partial f}{\partial x}(x_0,y_0), \frac{\partial f}{\partial y}(x_0,y_0)\right) \neq (0,0)$$

*Such a point is called a **non-singular** point on the curve . If every point on the curve is non singular then then we say our curve is non singular. A point which is not non-singular is called a **singular** point.*

Homogenization

The question still remains of how curves in $\mathbb{P}^2$ might be transformed into curves in $\mathbb{A}^2$. Such transformations are typically carried out through a process known as homogenization. Homogenization maps a curve E in $\mathbb{P}^2$ to a curve in $\mathbb{A}^2$ by transforming the function by which E is defined, $F(X;Y;Z)$ into a function $f(x,y)$. The process for such transformations is rather straightforward. We define $f(x,y)$ by the following relation :

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

In such a transformation, every homogeneous triple (a,b,c) that solves the polynomial F is scaled by the reciprocal of an element of the triple. For example, if the function F is to be homogenized with respect to Z, the solutions to F are scaled in the following way :

$$(a,b,c) \longmapsto \left(\frac{a}{c}, \frac{b}{c}, 1\right)$$

Note that, in projective space, the original triple and the triple to which it is mapped are equivalent because $\frac{1}{c}$ is a nonzero scalar applied to each element of the triple. Notice that $f(x,y) = \tilde{F}(x,y,1)$. So for dehomogenization of a polynomial $\tilde{F}(x,y,z)$ we have to substitute $z = 1$ to finding $f(x,y) = 0$.

Properties of homogeneous polynomial

Suppose that our polynomials have coefficients in a field K, and if $x,y,z \in \mathbb{K}$ such that $\tilde{F}(x,y,z) = 0$. Notice that

(1) For any $\lambda \in K, \tilde{F}(\lambda x, \lambda y, \lambda z) = \lambda^n \tilde{F}(x,y,z)$ (n = total degree of F)

(2) For any non zero $\lambda \in K, \tilde{F}(\lambda x, \lambda y, \lambda z) = 0$ iff $F(x,y,z) = 0$
In particular, for z we have $\tilde{F}(x,y,z) = 0$ iff $F(x/z, y/z) = 0$

Now we will discuss how to get all rational points on the conic and cubic then we will study about elliptic curve (particular cubic curve) .

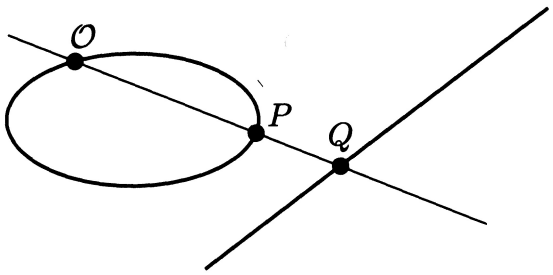
1.2 Rational points on conics

A line is said to be a **"rational"** if we can write its equation by rational coefficients i.e., $ax + by + c = 0$ is rational if

$$a, b, c \in \mathbb{Q}$$

We can easily check that two rational line intersect at a rational point and line passing through two rational points is rational

We will say that a conic $C : ax^2 + bxy + cy^2 + dx + ey + f = 0$ is rational if $a, b, c, d, e, f \in \mathbb{Q}$. Now we will describe all rational points on conic completely. Given a rational conic, the first question is whether or not there are any rational points on it. But let us suppose that there is one rational point $\mathcal{O}$ on our rational conic then we can get all of them very simply. We just draw some rational line L and we project the conic onto the line from this point O and for $\mathcal{O}$ itself onto the line given by the figure 1.4, we use the tangent line to the conic at $\mathcal{O}$. A line meets a conic in two points, so for every point P on the conic we get a point



Projecting a Conic onto a Line

Figure 1.4:

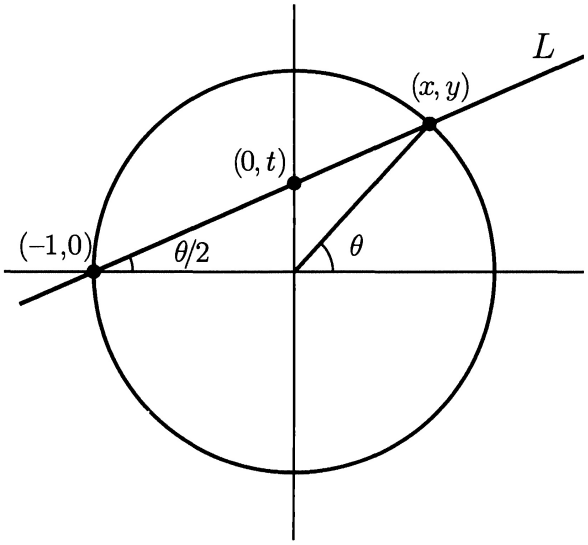
Q on the line; and conversely, for every point Q on the line, by joining it to the point $\mathcal{O}$, we get a point P on the conic. We get a one-to-one correspondence between the points on the conic and points on the line . If the point P on the conic has rational coordinates, then the point Q on the line will have rational coordinates because we know line passing through two rational points is rational and intersection point of two rational line is rational. And conversely, if Q is rational, then the line through P and Q meets the conic in two points if one of which is rational So the other point is rational. Thus the rational points on the conic are in one-to-one correspondence with the rational points on the line. Of course, the rational points on the line are easily described in terms of rational values of some parameter . We will try this procedure for the unit circle :

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

We will project from the point $(-1, 0)$ onto the y - axis. Let's call the point of intersection $(0, t)$ given by the following figure 1.5 on page. we can easily find t by x and y and by simple calculation we get :

$$x = \frac{1 - t^2}{1 + t^2} \quad , \quad y = \frac{2t}{1 + t^2}.$$

This is the rational parametrization of the circle and now the assertion made above is clear from these formulas. i.e. if x and y are rational numbers, then t will be a rational number and vice versa. So this is the way for getting all rational points on the circle by all choice of t. That will give us all points except $(-1, 0)$ and for $(-1, 0)$ substitute infinity for t .



A Rational Parametrization of the Circle

Figure 1.5:

Problem 1.2.1. *Show that there is no rational point on the circle :*

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

.

Proof. suppose there is a rational point (x, y) then we can write it as

$$x = \frac{X}{Z}, \qquad y = \frac{Y}{Z}$$

for some integers X, Y, Z which have no common factor. It follows that both X and Y are not divisible by 3. This is true because if $3|X$, then $3|Y^2 (= 3Z^2 - X^2)$ so $3|Y$. But then 9 divides $X^2 + Y^2 = 3Z^2$, so $3|Z$, contradicting the fact that X, Y, Z have no common factors. Hence 3 does not divide X, and similarly for Y. Since X and Y are not divisible by 3, we have

$$X \equiv \pm 1 \mod 3, \qquad Y \equiv \pm 1 \mod 3, \qquad X^2 \equiv Y^2 \equiv 1 \mod 3$$

But then

$$0 \equiv 3Z^2 = X^2 + Y^2 \equiv 1 + 1 \equiv 2 \qquad \mod 3$$

This contradiction shows that no two rational numbers have squares which add up to 3. □

1.3 Geometry of cubic curves

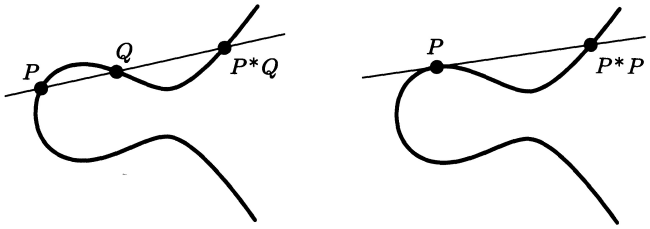
Let

$$ax^3 + bx^2y + cxy^2 + dy^3 + ex^2 + fxy + gy^2 + hx + iy + j = 0$$

be equation for general cubic over field K.

We can not use the geometric principle that worked so well for conic because a line generally meets a cubic in three points. If we have one rational point, we cannot project the cubic onto a line, because each point on the line would then correspond to two points on the curve

But there is a geometric principle we can use. If we can find two rational points on the curve, then we can generally find a third one. Namely, draw the line connecting the two points you have found. This will be a rational line, and it meets the cubic in one more point. If we look and see what happens when we try to find the three intersections of a rational line with a rational cubic, we find that we come out with a cubic equation with rational coefficients. If two of the roots are rational, then the third must be also. We will work out some explicit examples below, but the principle is clear. So this gives some kind of composition law : starting with two points P and Q and let $P * Q$ denote the third point of intersection of the line with the cubic given by the following figure 1.6. Even if we only have one rational point P, we can still generally



The Composition of Points on a Cubic

Figure 1.6:

get another. By drawing the tangent line to the cubic at P, we are essentially drawing the line through P and P . The tangent line meets the cubic twice at P, and the same argument will show that the third intersection point is rational. Then we can join these new point up and get more points. So if we start with a few rational points, then by drawing lines, we generally get lots of others.

It is very difficult to determine in finite number of steps whether a given rational cubic has a rational point. We will leave this difficult problem aside, and assume that we have a cubic which has a rational point $\mathcal{O}$

If we consider the set of all rational points on the cubic, we can say that set has a law of composition. Given any two points P, Q, we have defined a third point $P * Q$. We might ask about the algebraic structure of this set and this composition law; for example, is it a group ? Unfortunately, it is not a group; to start with, it is fairly clear that there is no identity element.

We can make it into a group in such a way that the given a rational point $\mathcal{O}$ becomes the zero element of the group. We will denote the group law by $+$ because it is going to be a commutative group. The rule is as follows :

To add P and Q, take the third intersection point $P * Q$, join it to $\mathcal{O}$ (zero element), and then take the third intersection point to be $P + Q$. Thus by definition, $P + Q = \mathcal{O} * (P * Q)$

In the following figure 1.7, 1.8, 1.9 we can understand geometrically our group law.

We also want to mention that there is nothing special about our rational point $\mathcal{O}$; if we choose different $\mathcal{O}'$ to be the zero element of our group,then we get a group with exactly same structure. In fact the map

$$P \longmapsto P + (\mathcal{O}' - \mathcal{O})$$

is an isomorphism from the group "C with zero element $\mathcal{O}$ to the group "C with the zero element $\mathcal{O}'$.

1.4 Elliptic curve

Definition 1.4.1. *An **elliptic curve** is a pair $(E, \mathcal{O})$,where E is a non singular curve and $\mathcal{O} \in E$ in projective space (We generally denote the elliptic curve by E , the point $\mathcal{O}$ being understood.) The elliptic curve E is defined over field K, written E/K, if E is defined over field K as a curve and $\mathcal{O} \in E$*

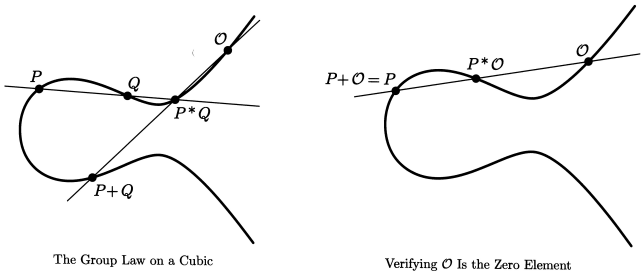


Figure 1.7:

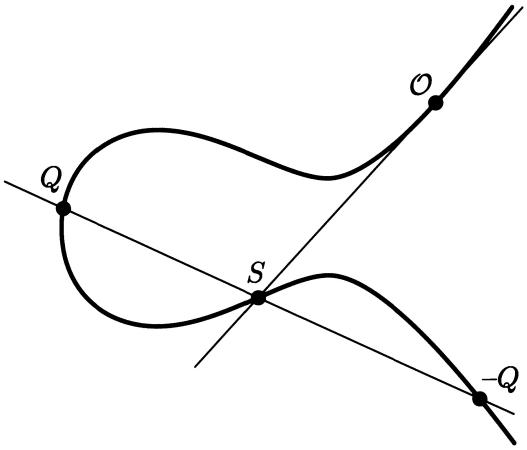


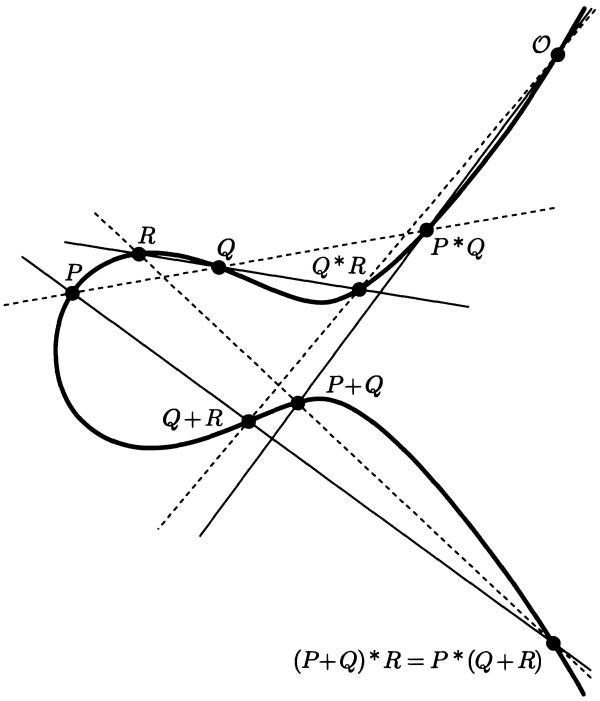
Figure 1.8:

Why have we concentrated attention only on the non-singular cubics? The singular cubics (1.10) and the non-singular cubics have completely different types of behavior. For instance, the singular cubics are just as easy to treat as conics. If we project from the singular point onto some line, we see that the line going through that singular point meets the cubic twice at the singular point, so it meets the cubic only once more. The projection of the cubic curve onto the line is thus one-to-one. So just like a conic, the rational points on a singular cubic can be in one-to-one correspondence with the rational points on the line. In fact, it is very easy to do that explicitly with formulas.

If we let $r = \frac{y}{x}$, then the equation $y^2 = x^2(x+1)$ becomes

$$r^2 = x + 1 \qquad \text{and so} \qquad x = r^2 - 1 \qquad \text{and} \qquad y = r^3 - r$$

. These operation are inverse of each other, and are defined at all rational points except for the singular point $(0, 0)$ on the curve. So the singular cubics are trivial to analyze as far as rational points go. But one can prove that and Mordell's theorem does not hold for them means this group is not finitely generated.



Verifying the Associative Law

Figure 1.9:

1.5 Weierstrass equations

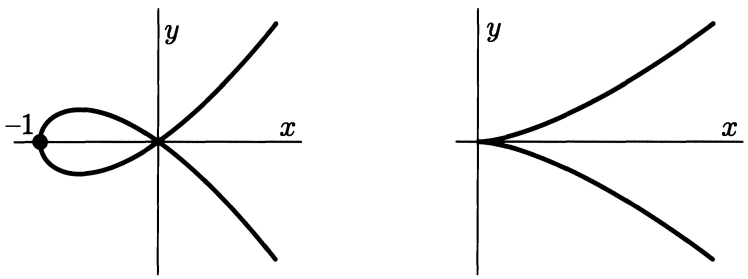
In this section we will transform our elliptic curve into simplified cubic equation known as Weierstrass equation for an elliptic curve which will help to study more about elliptic curve

Weierstrass equations is a projective cubic curve of the form

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3$$

with an extra point $\mathcal{O}' = [0, 1, 0]$ over field K. After dehomogenization by substituting $x = X/Z$ and $y = Y/Z$ Weierstrass equations becomes :

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



A Singular Cubic with Distinct Tangent Directions

A Singular Cubic with A Cusp

Figure 1.10:

There is the extra point at infinity $\mathcal{O}' = [0, 1, 0]$ on this elliptic curve . As usual,if $a_1, \ldots, a_6 \in K$, then E is said to be defined over field K.

By Riemann-Roch theorem We know that every elliptic curve can be written as a Weierstrass plane cubic, and conversely, every non-singular Weierstrass plane cubic curve is an elliptic curve.

Proposition 1.5.1. *[ST92, Prop.3.1] Let E be an elliptic curve defined over field K*

(a) There exist functions $x, y \in E(K)$ such that the map

$$\phi : E \to \mathbb{P}^2, \qquad \phi = [x, y, 1]$$

gives an isomorphism of E/K onto a curve given by a Weierstrass equation.

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3$$

satisfying $\phi(\mathcal{O}) = [0, 1, 0]$

(b) Any two Weierstrass equations for E as in (a) are related by a linear change of variables of the form

$$x = u^2x' + r \qquad \text{and} \qquad y = u^3y' + u^sx' + t$$

where $u, r, s, t \in K$ and $u \neq 0$.

If $\text{char}(K) \neq 2$, then we can simplify the equation by completing the square. Thus the substitution

$$y \longmapsto \frac{1}{2}(y - a_1x - a_3)$$

gives an equation of the form

$$E : y^2 = 4x^3 + b_2x^2 + 2b_4x + b_6$$

where

$$b_2 = a_1^2 + 4a_2, \qquad b_4 = 2a_4 + a_1a_3, \qquad b_6 = a_3^2 + 4a_6$$

We also define quantities :

$$\begin{aligned} b_8 &= a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2 \\ c_4 &= b_2^2 - 24b_4 \\ c_6 &= -b_2^3 + 36b_2b_4 - 216b_6 \\ \triangle &= -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6 \\ j &= \frac{c_4^3}{\triangle} \end{aligned}$$

Definition 1.5.2. *The quantity $\triangle$ is known as discriminat of the polynomial $f(x) = 4x^3 + b_2x^2 + 2b_4x + b_6$ and j is known as j-invariant of elliptic curve.*

Definition 1.5.3. *The discriminant of cubic $f(x)$ is the quantity :*

$$\triangle = (\alpha_1 - \alpha_2)^2(\alpha_1 - \alpha_3)^2(\alpha_2 - \alpha_3)^2$$

Proposition 1.5.4. **(a)** *The elliptic curve given by a Weierstrass equation is non singular if and only if $\triangle \neq 0$*

(b) *Two elliptic curves are isomorphic over field $\bar{K}$ if and only if they both have the same j-invariant.*

Proof. **(a)** Let C be given by the Weierstrass equation in projective space:

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

We will check that the point at infinity $\mathcal{O} = [0,1,0]$ is never singular.
Since

$$\frac{\partial F}{\partial Z}(\mathcal{O}) = 1 \neq 0$$

For simplification we assume $\text{char}(K) \neq 2$ then we can convert our C as:

$$C : y^2 = 4x^3 + b_2x^2 + b_4x + b_6$$

The curve C is singular if and only if there ia a point $(x_0, y_0) \in C$ satisfying

$$2y_0 = 12x_0^2 + 2b_2x_0 + 2b_4 = 0 \Rightarrow y_0 = 0$$

So the singular points are exactly the points of the form $(x_0, 0)$ such that x_0 is a double root of the polynomial $4x^3 + b_2x^2 + 2b_4x + b_6$. This polynomial has double root if and only if discriminant, which equals $16\triangle$, vanishes.

(b) We will see that after changing the variables given be proposition 1.5.1 (b) in following way fixing $[0,1,0]$ we get same j-invariant.

$$x = u^2x' + r \text{ and } y = u^3y' + u^2sx' + t$$

where $u, r, s, t \in K$ and $u \neq 0$.

$$\begin{aligned}
x^2 &= (u^2x' + r)^2 = u^4x'^2 + r^2 + 2ru^2x' \\
x^3 &= u^6x'^3 + r^3 + 3ru^4x'^2 + 3r^2u^2x' \\
y^2 &= (u^3y' + u^2sx' + t)^2 = u^6y'^2 + u^4s^2x'^2 + t^2 + 2u^5sx'y' + 2u^stx' + 2u^3ty' \\
xy &= u^5x'y' + u^4sx'^2 + u^2tx' + tx' + u^3ry' + u^2srx' + rt
\end{aligned}$$

Now substitute these values in equation in Weierstrass equation for an elliptic curve, then we get :

$$\begin{aligned}
f(x',y') = {} & u^6y'^2 + u^4s^2x'^2 + t^2 + 2u^5sx'y' + 2stu^2x' + 2tu^3y' + a_1u^5x'y' + a_1u^4sx'^2 \\
& + a_1u^2tx' + a_1u^3ry' + a_1u^2srx' + a_1rt + a_3u^3y' + a_3u^2sx' + a_3t - u^6s'^3 \\
& - r^3 - 3ru^4x'^2 - 3r^2u^2x' - a_2u^4x'^2 - a_2r^2 - 2a_2ru^2x' - a_4u^2x' - a_4r \\
& - a_6 = 0 \\
f'(x',y') = {} & y'^2 + \frac{1}{u}(a_1 + 2s)x'y' + \frac{1}{u^3}(2t + ra_1a_3)y' - x^3 + \frac{1}{u^2}(s^2 + a_1s - 3r - a_2)x'^2 \\
& + \frac{1}{u^4}(2st + a_1t + a_1sr + a^3s - 3r^2 - 2a_2r - a_4)x' + \frac{1}{u^6}(a_1rt + a_3t - r^3 \\
& - a_2r^2 - a_4r - a_6) = 0
\end{aligned}$$

Now calculation for b'_2, b'_4, b'_6 and b'_8

$$
\begin{aligned}
b'_2 &= a'_1 + 4a'_2 = \frac{1}{u^2}(a_1 + 2s)^2 + \frac{4}{u^2}(a_2 - sa_1 + 3r - s^2) \\
&= a_1^2 + 4s^2 + 4a_1 s + 4a_2 - 4sa_1 + 12r - 4s^2 \\
u^2 b'_2 &= a_1^2 + 4a_2 + 12r \Rightarrow u^2 b'_2 = b_2 + 12r \\
b'_4 &= 2a'_4 + a'_1 a'_3 \\
&= \frac{2}{u^4}(a_4 - sa_3 + 2ra_2 - ta_1 - ra + 1s + 3r^2 - 2st) + \frac{1}{u}(a_1 + 2s)\frac{1}{u^3}(a_3 + ra_1 + 2t) \\
&= 2a_4 - 2sa_3 + 4ra_2 - 2ta_1 - 2ra_1 s + 6r^2 - 4st + a_1 a_3 + ra_1^2 + 2a_1 t + 2sa_3 + 2sra_1 + 4st. \\
u^4 b'_4 &= 2a_4 + 4a_2 + 6r^2 + ra_1^2 + a_1 a_3 = 2a_4 + a_1 a_3 + r(4a_2 + a_1^2) + 6r^2 \\
u^4 b'_4 &= b_4 + rb_2 + 6r^2
\end{aligned}
$$

$$
\begin{aligned}
b'_6 &= a'^2_3 + 4a'_6 \\
&= \frac{1}{u^6}(a_3 + ra_1 + 2t)^2 + \frac{4}{u^6}(a_6 + ra_4 + r^2 a_2 + r^3 - ta_3 - t_r^2 ta_1 \\
u^6 b'_6 &= a_3^2 + r^2 a_1^2 + 4t^2 + 2ra_1 a_3 + 4ra_1 t + 4ta_3 + 4a_6 + 4ra_4 + 4r^2 a_2 + 4r^3 - 4ta_3 - 4t^2 \\
&\quad - 4rta_1 \\
&= a_3^2 + r^2 a_1^2 + 2ra_1 a_3 + 4a_6 + 4ra_4 + 4r^2 a_2 + 4r^3 \\
&= a_3^2 + 4a_6 + 2r(2a_4 + a_1 a_3) + r^2(a_1^2 + 4a_2) + 4r^3 \\
u^6 b'_6 &= b_6 + 2rb_4 + r^2 b_2 + 4r^3 \\
b'_8 &= a_1^2 a'_6 + 4a'_2 a'_6 - a'_1 a'_3 a'_4 + a'_2 a'^2_3 - a'^2_4 \\
&= \frac{1}{u^2}(a_1 + 2s)^2 \frac{1}{u^6}(a_6 + ra_4 + r^2 a_2 + r_t^3 a_3 - t^2 - rta_1) + \frac{4}{u^2}(a_2 - sa_1 + 3r - s^2) \\
&\quad \frac{1}{u^6}(a_6 + ra_4 + r^2 a_2 + r^3 - ta_3 - t^2 - rta_1) - \frac{1}{u}(a_1 + 2s)\frac{1}{u^3}(a_3 + ra_1 + 2t) \\
&\quad \frac{1}{u^4}(a_4 - sa_3 + 2ra_2 - ta_1 - rsa_1 + 3r^2 - 2st) + \frac{1}{u^2}(a_2 - sa_1 + 3r - s^2) \\
&\quad \frac{1}{u^6}(a_3 + ra_1 + 2t)^2 - \frac{1}{u^8}(a_4 - sa_3 + 2ra_2 - ta_1 - rsa_1 + 3r^2 - 2st)^2 \\
&= \frac{1}{u^8}(a_1^2 + 4s^2 + 4a_1 s)(a_6 + ra_4 + r^2 a_2 + r_t^3 a_3 - t^2 - rta_1) + \frac{4}{u^8}(a_2 - sa_1 + 3r - s^2) \\
&\quad (a_6 + ra_4 + r^2 a_2 + r^3 - ta_3 - t^2 - rta_1) - \frac{1}{u^8}(a_1 a_3 + ra_1^2 + 2ta_1 + 2sa_3 + 2sra_1 \\
&\quad + 4st)(a_4 - sa_3 + 2ra_2 - ta_1 - rsa_1 + 3r^2 - 2st) + \frac{1}{u^8}(a_2 - sa_1 + 3r - s^2) \\
&\quad (a_3^2 + r^2 a_1^2 + 4t^2 + 2a_1 a_3 r + 4a_1 rt + 4a_3 t) - \frac{1}{u^8}((a_4 - sa_3)^2 + (2ra_2 - ta_1)^2 + \\
&\quad (3r^2 - rsa_1 - 2st)^2 + 2(a_4 - sa_3)(2ra_2 - ta_1) + 2(2ra_2 - ta_1)(3r^2 - rsa_1 - 2st) \\
&\quad + 2(3r^2 - rsa_1 - 2st)(a_4 - sa_3)) \\
&= a_1 a_6 + 4a_2 a_6 - a_1 a_3 a_4 + a_2 a_3^2 - a_4^2 + 3r(a_3^2 + 4a_6) + 3r^2(2a_4 + a_1 a_3) + r^3(a_1^2 + 4a_4) \\
&\quad + 3r^4 \\
&= b_8 + 3rb_6 + 3r^2 b_4 + r^3 b_2 + 3r^4
\end{aligned}
$$

Now we will see after change of variable which quantities are changing and what is invariant by the following table.

$$
\begin{aligned}
ua_1' &= a_1 + 2s \\
u^2a_2' &= s^2 + a_1s - 3r - a_2 \\
u^3a_3' &= 2t + ra_1a_3 \\
u^4a_4' &= 2st + a_1t + a_1sr + a^3s - 3r^2 - 2a_2r - a_4 \\
u^6a_6' &= a_1rt + a_3t - r^3 - a_2r^2 - a_4r - a_6 \\
u^2b_2' &= b_2 + 12r \\
u^4b_4' &= b_4 + rb_2 + 6r^2 \\
u^6b_6' &= b_6 + 2rb_4 + r_2^b + 4r^3 \\
u^8b_8' &= b_8 + 3rb_6 + 3r^2b_4 + r^3b_2 + 3r^4 \\
u^4c_4' &= c_4 \\
u^6c_6' &= c_6 \\
u^{12}\triangle' &= \triangle \\
j' &= j
\end{aligned}
$$

So after change of variable up to isomorphism we got same j-invariant.
For converse, we will assume $\mathrm{char}(k) \neq 2, 3$. Let E and E' be two elliptic curves over field K with the same j-invariant in form of Weierstrass equation:

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

$$E' : y'^2 = x'^3 + A'x' + B'$$

From the assumption $j(E) = j(E')$ implies that

$$\frac{(4A)^3}{4A^3 + 27B^2} = \frac{(4A')^3}{4A'^3 + 27B'^2}$$

So

$$A^3B'^2 = A'^3B^2$$

We look for an isomorphism of the form $(x, y) = (u^2x', u^3y')$ and we will discuss isomorphism in three cases:
Case(1 :) $A = 0 (j = 0)$. Then $B \neq 0$, since $\triangle \neq 0$, so $A' = 0$, and we obtain an isomorphism using $u = (B/B')^{1/6}$.
Case(2 :) $B = 0 (j = 1728)$. Then $A \neq 0$, so $B' = 0$, and we obtain an isomorphism using $u = (A/A')^{1/4}$.
Case(3 :) $AB \neq 0 (j = 0, 1728)$. Then $A'B' \neq 0$, since one of them were 0, then both of them would be 0, contradicting $\triangle' \neq 0$. Taking $u = (A/A')^{1/4} = (B/B')^{1/6}$ gives the desired isomorphism.

□

1.6 Legendre form

Just from j-invariants of elliptic curves we can know they are isomorphic are not. So j-invariant is very important quantity about elliptic curves. Now we will discuss **Legendre form** of the elliptic curve where we can find j- invariant explicitly. A Weierstrass equation is in Legendre form if it can be written as :

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

over algebraic closed field K.

Proposition 1.6.1. *Let $E : y^2 = x^3 + ax^2 + bx + c$ be an elliptic curve over $\bar{K}$ in Weierstrass form then we can transform elliptic curve E into Legendre form.*

Proof. Let $y^2 = x^3 + ax^2 + bx + c$ be an elliptic curve over $\bar{K}$ in Weierstrass form . If α_1, α_2 and α_3 are the roots of the polynomial. Then $y^2 = (x - \alpha_1)(x - \alpha_2)(x - \alpha_3)$ Replace x by $(\alpha_2 - \alpha_1)x' + \alpha_1$ and y by $(\alpha_2 - \alpha_1)^{3/2}y')$ we get :

$$\begin{aligned}
(\alpha_2 - \alpha_1)^{3/2}y')^2 &= ((\alpha_2 - \alpha_1)x' + \alpha_1 - \alpha_1)((\alpha_2 - \alpha_1)x' + \alpha_1 - \alpha_2)((\alpha_2 - \alpha_1)x' + \alpha_1 - \alpha_3) \\
(\alpha_2 - \alpha_1)^3y'^2 &= (\alpha_2 - \alpha_1)x'((\alpha_2 - \alpha_1)x' - (\alpha_2 - \alpha_1))((\alpha_2 - \alpha_1)x' - (\alpha_3 - \alpha_1)) \\
(\alpha_2 - \alpha_1)^3y'^2 &= (\alpha_2 - \alpha_1)^3x'(x' - 1)(x' - \frac{\alpha_3 - \alpha_1}{\alpha_2 - \alpha_1}) \\
E_\lambda : y'^2 &= x'(x' - 1)(x' - \lambda) \qquad \text{where } \lambda = \frac{\alpha_3 - \alpha_1}{\alpha_2 - \alpha_1}
\end{aligned}$$

□

Proposition 1.6.2.

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

Proof. On comparing E_λ with Weierstrass equation

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

over field K then we get :

$$a_1 = 0, \qquad a_3 = 0, \qquad a_2 = -(\lambda + 1), \qquad a_4 = \lambda, \qquad a_6 = 0$$

So value of $b_2, b_4, b_6, b_8, c_4, \triangle, j$ will be :

$$
\begin{aligned}
b_2 &= -4(\lambda+1) \\
b_4 &= 2\lambda \\
b_6 &= 0 \\
b_8 &= \lambda^2 \\
c_4 &= 16(\lambda^2-\lambda+1) \\
\triangle &= 16\lambda^2(\lambda-1)^2 \\
j &= \frac{(16(\lambda^2-\lambda+1))^3}{16\lambda^2(\lambda-1)^2}
\end{aligned}
$$

Hence j-invariant of E_λ is

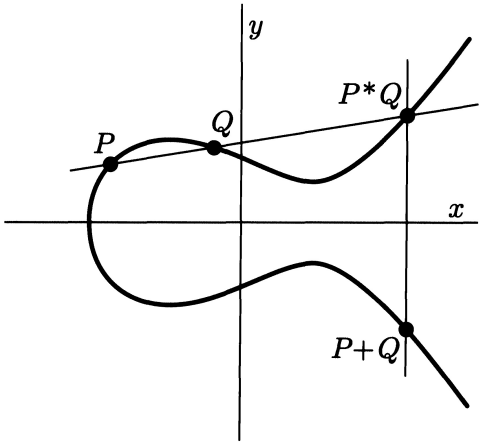
$$j(E_\lambda) = \frac{2^8(\lambda^2-\lambda+1)^3}{\lambda^2(\lambda-1)^2}$$

□

Now we are going to define compostion law for rational points on elliptic curve in Weierstrass form.

Composition law on cubic curves

Starting with two points P and Q , we draw the line through P and Q and let $P * Q$ denote the third point of intersection of the line with the cubic. Even if we only have one rational point P, we can still get another. By drawing the tangent line to the cubic at P, we are essentially drawing the line through P and P. The tangent line meets the cubic twice at P, and we can't use the same geometric principle that worked so well for conics because a line generally meets a cubic in three points And if we have one rational point, we can't project the cubic onto a line, because each point on the line would then correspond to two points on the curve. argument will show that the third intersection point is rational. Then we can join these new points up and get more points. So if we start with a few rational points, then by drawing lines, we generally get lots of others.



Adding Points on a Weierstrass Cubic

1.7 Explicit formulas for the group law

We start with our equation for the elliptic curve over field K :

$$E : y^2 = f(x) = x^3 + ax^2 + bx + c$$

Let $P_1 = (x_1, x_2)$ and $P_2 = (x_2, y_2)$ We may define $P_1 + P_2 = P_3$, where $P_3 = (x_3, y_3)$. From this construction, it follows that $P_1 + P_2 = (x_3, y_3)$. We define the line connecting P_1, P_2, and P_3 as :

$$y = \lambda x + v; \text{ where } \lambda = \tfrac{y_2 - y_1}{x_2 - x_1} \text{ and } v = y_1 - \lambda x_1 = y_2 - \lambda x_2.$$

We can substitute the equation for this line into the equation for E, so we have $(\lambda x + v)^2 = x^3 + ax^2 + bx + c$. Moving everything to one side and expanding, we get :

$$0 = x^3 + ax^2 + bx + c - (\lambda^2 x^2 + v^2 + 2\lambda v x).$$

After some factoring, this yields :

$$0 = x^3 + (a - \lambda^2)x^2 + (b - 2v\lambda)x + (c - v^2)$$

The roots of this equation are $x_1; x_2$, and x^3, so we can rewrite the left side :

$$(x - x_1)(x - x_2)(x - x_3) = x^3 + (a - \lambda^2)x^2 + (b - 2v\lambda)x + (c - v^2).$$

So we have that $\lambda^2 - a = x_1 + x_2 + x_3$. We can use this to find formulas for x_3 and y_3

$$x_3 = \lambda^2 - a - x_1 - x_2 \qquad \text{and} \qquad y_3 = \lambda x_3 + v$$

This equation is called the duplication formula. This is a useful result because it allows us to find the coordinates of $P_1 + P_2$ given distinct points P_1 and P_2 on an elliptic curve. To find $P_1 + P_2$, all we have to do is use the duplication formula to find the coordinates of P_3, and then reflect over the x-axis by taking the opposite of y_3.

Duplication formula

The formulas we gave earlier involve the slope λ of the line connecting the two points. So suppose that we have $P_0 = (x_0, y_0)$ and we want to find $P_0 + P_0 = 2P_0$. We need to find the line joining P_0 to P_0. Because $x_1 = x_2$ and $y_1 = y_2$, we can't use our formula for λ. But the recipe we described for adding a point to itself says that the line joining P_0 to P_0 is the tangent line to the cubic at P_0. From the relation $y^2 = f(x)$ we find by implicit differentiation that

$$\lambda = \frac{dy}{dx} = \frac{f'(x)}{2y}$$

Sometimes it is convenient to have an explicit expression for $2P$ in terms of the coordinates for P. If we substitute $\lambda = \frac{f'(x)}{2y}$ into the formulas given earlier, put everything over a common denominator, and replace y^2 by $f(x)$, then we find that

$$x(2P) = \frac{x^4 - 2bx^2 - 8cx + b^2 - 4ac}{4x^3 + 4ax^2 + 4bx + 4c}$$

1.8 Group structure

Now we will show that the set of points on an elliptic curve, combined with the binary relation $+$ on the curve, forms an Abelian group. We will prove each condition for the group structure independently.

Closure

Closure property is clear by the definition of construction.

Associative law

We will use Bezout's theorem to demonstrate this result, particularly in showing that for any three rational points on an elliptic curve, denoted P, Q and R, we have that $(P + Q) + R = P + (Q + R)$. We shall assert Bezout's theorem, and use this result to prove a more specific theorem about cubics. It is then rather simple to prove that associativity holds for the group structure on an elliptic curve.

Theorem 1.8.1 (Bezout's Theorem)**.** *For any two polynomials C_1 and C_2 that do not have a component in common, where C_1 has degree n and C_2 has degree m, C_1 and C_2 intersect at nm distinct points.*

Lemma 1.8.2. *For any three cubic curves C_1, C_2, C_3 in projective space, where C_1 and C_2 do not have a component in common, if C_3 passes through eight of the nine intersection points of C_1 and C_2, then C_3 also passes through the ninth intersection point.*

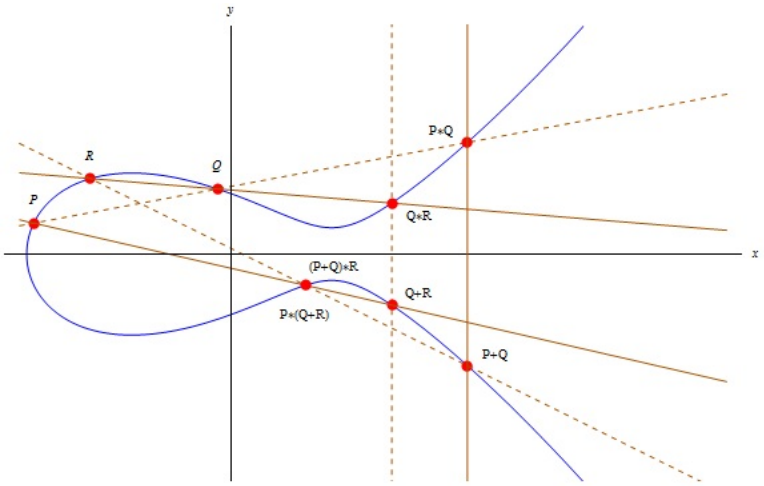
Proof. Let C_1 and C_2 be two cubic curves. Bezout's theorem gives us that C_1 and C_2 intersect at 9 distinct points. Assume that C_3 passes through 8 of the 9 intersection points of C_1 and C_2. Because C_1 and C_2 are defined in projective space, they are associated with two functions F_1 and F_2 such that $C_1 : F_1(X, Y, Z) = 0$ and $C_2 : F_2(X, Y, Z) = 0$. It is therefore possible to create a linear combination of F_1 and F_2, defined by $\lambda F_1 + \lambda F_2$ for some values of λF_1 and λF_2. Because such a linear combination is defined in projective space, it forms a one-dimensional family. Because C_3 is pinned down by 8 points through which it must travel, it is part of a one-dimensional family. Thus, for some values of λF_1 and λF_2 , we have $F_3 = \lambda F_1 + \lambda F_2$ for $C_3 : F_3(X, Y, Z)$. If we are to evaluate this relationship at the ninth intersection point of C_1 and C_2, we have $F_1 = F_2 = 0$ by definition. Thus, $F_3 = 0$ at this point, and therefore, C_3 passes through the ninth point of intersection. □

We can now use Bezout's theorem to prove the associativity property for the group operation $+$ on the points on an elliptic curve. To show that $P + (Q + R) = (P + Q) + R$, it suffices to show that $P * (Q + R) = (P + Q) * R$, because this point will simply be reflected over the x-axis to obtain the desired result.

Claim :
For any three points P, Q, R on an elliptic curve $E, P * (Q + R) = (P + Q) * R$.

Proof. Let P, Q, R be points on an elliptic curve E. We will now give names to the lines used in defining the relevant points on E :
Let L_1 be the line passing through P, Q and $P * Q$.
Let L_1' be the line passing through Q, R, and $Q * R$.
Let L_2 be the vertical line passing through $O, Q * R$ and $Q + R$.
Let L_2' be the vertical line passing through $O, P * Q$ and $P + Q$.
Let L_3 be the line passing through $P + Q$ and R.
Let L_3' be the line passing through P and $Q + R$.
Because C is a projective curve, the lines L_3 and L_3' must intersect at a single point,denoted A. Furthermore, because both L_3 and L_3' are lines through two points on C, they must intersect C at a third point. Thus, if A lies on the elliptic curve, then $A = P * (Q + R) = (P + Q) * R$ and the associative property holds. Let D be the set consisting of P, Q, R, the compositions $P * Q$ and $Q * R$, the additions $P + Q$ and $Q + R$, and the point A. By construction, every point $p \in D$ has both a line L_i and a line L_i' passing through it. We may define $C_1 = L_1 * L_2 * L_3$ and let $C_2 = L_1' * L_2' * L_3'$, so C_1 and C_2 both pass through all of the nine points $p \in D$.

By definition, the elliptic curve E passes through the eight points $p \in (D/A)$, so E passes through A by above Lemma, and the associative property holds. □

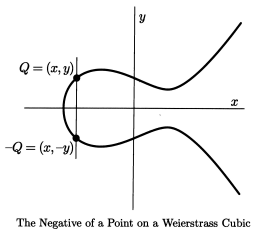


Zero element

The identity element for the binary operation $+$ is the point at infinity, $\mathcal{O}$. This property is rather clear intuitively. Recall that for all points P and Q on the elliptic curve, $P + Q = O * (P * Q)$. Thus, for any point P on the elliptic curve, $\mathcal{O} + P = \mathcal{O} * (\mathcal{O} * P)$. The right side of this equation reflects the point P over the x-axis twice, resulting in the point P. Thus,$\mathcal{O} + P = P$, and there is an identity element for the group.

Inverse of a point

The property that every point Q on the elliptic curve must have an inverse is also rather clear to prove intuitively. For any point Q on the elliptic curve, we define $-Q$ to be the point on the elliptic curve obtained by reflecting Q over the x-axis. Thus, $Q * (-Q)$ must be the point at infinity, implying that $Q + (-Q) = \mathcal{O}$ and, therefore, that the inverse property holds.



The Negative of a Point on a Weierstrass Cubic

Commutativity

Commutativity is very clear from the definition of composition law because line joining P and Q is same as line joining Q and P

Hence set of all rational point points on elliptic curve $E(\mathbb{Q})$ with point at infinity $\mathcal{O}$ is Abelian group.

Chapter 2

Points of finite order

In this chapter our aim is to prove Nagell-Lutz theorem which says that $(x, y) \in E(\mathbb{Q})_{\text{tor}}$ must have integer coordinate and y is 0 or y divides the discriminant. In this theorem we are using discriminant and points of finite order so also we will define discriminant of the polynomial and how looks like torsion subgruop of $E(\mathbb{Q})$. So from the theorem we can conlude that we can find $(x, y) \in E(\mathbb{Q})_{\text{tor}}$ in finite number step because the set of all divisors of discriminant is finite.

2.1 Points of order two and three

Definition 2.1.1. *A point P of any group is said to be of order $n \in \mathbb{N}$ if*

$$nP = P + P + \cdots + P = 0$$

but $mP \neq 0$ for $1 \leq m < n$. If such m does not exist then we say it has infinite order.

Now we will discuss about points of finite order of elliptic curves given in Weierstrass form : $y^2 = f(x) = x^3 + ax^2 + bx + c$ over the field K and here we are considering point at infinity as zero element for the group law of elliptic curve.

Points of order two

Let P be a non zero element of our group i.e., $2P = 0 \Rightarrow P = -P$ and we know if $P = (x, y)$ then $-P = (x, -y)$ so y co-ordinate of the points of order two will be zero. Let x_1, x_2 and x_3 are the roots of the polynomial $f(x)$. If P_1, P_2 and P_3 are the points of order two.then
$P_1 = (x_1, 0), P_2 = (x_2, 0)$ and $P_3 = (x_3, 0)$. If we allow complex root x_1, x_2 and x_3 of the polynomial $f(x)$ then these are exactly three.If we take all these points of order two with zero element 0 of elliptic curve then the set $\{\mathcal{O}, P_1, P_2, P_3\}$ form a subgroup. So we have a group of order four which means if we add two non zero elements of this group we get third one i.e., these three points are collinear.And we have Abelian group of order four so it is direct product of two cyclic group of order two.

Points of order three

Let $P = (x, y)$ be a point of order three i.e.,

$$\begin{aligned} &3P = \mathcal{O} \Rightarrow 2P = -P \\ &\Rightarrow x(2P) = x(-P) = x(P) \\ &\Rightarrow \frac{x^4 - 2bx^2 - 8cx + b^2 - 4ac}{4x^3 + 4ax^2 + 4bx + 4c} = x \\ &\Rightarrow g(x) = 3x^4 + 4ax^3 + 6bx^2 + 12cx + (4ac - b^2) = 0 \end{aligned}$$

and conversely, if $P \neq \mathcal{O}$ and $x(2P) = x(P)$,then $2P \pm P \Rightarrow 3P = \mathcal{O}$. So the points of order three are exactly the points satisfying $x(2P) = x(P)$.

Remark : C has exactly nine points of order dividing 3. These nine points form a group which is a product of two cyclic groups of order three.

Proof : Let $P = (x, y)$ be any point of order three then $x(2P) = x(P)$, we know that x co-ordinate of $2P = \frac{f'(x)^2}{4f(x)} - a - 2x$ and we get :
$g(x) = 2f(x)f''(x) - f'(x)^2$ for checking all four roots(complex) of $g(x)$ are distinct we have to show that $g(x)$ and $g'(x)$ have no common roots. Suppose $g(x)$ and $g'(x)$ have common roots then

$$2f(x)f''(x) - f'(x)^2 \qquad \text{and} \qquad 2f(x)f'''(x) = 12f(x)$$

have common root if x is common root of $g(x)$ and $g'(x)$. So x would be common root of $f(x)$ and $f'(x)$ .So we got contradiction because elliptic curve E is non singular.Hence $g(x)$ has four distinct complex roots. Let $\beta_1, \beta_2, \beta_3, \beta_4$ be the four complex roots of $g(x)$ and for each β_i we have $\lambda_i = \sqrt{f(\beta_i)}$ and $\lambda_i \neq 0$ (because order of $(\beta_i, 0) = 2$). Then set $\{(\beta_1, \pm\lambda_1), (\beta_2, \pm\lambda_2), (\beta_3, \pm\lambda_3), (\beta_4, \pm\lambda_4)\}$ contains all points of order three of the elliptic curve. So this set with zero element of elliptic curve form an Abelian group of order nine having elements of order dividing three.We note that there is only one Abelian group with nine elements such that every element has order dividing three, namely, the product of two cyclic groups of order three.

2.2 Complex points on elliptic curves

We know by the geometry of elliptic curve $E : y^2 = x^3 + ax^2 + bx + c$ over field K have one or two components, depending on the real roots of $f(x)$. The points on the curve with complex coordinates form a group. The points with real coordinates form a subgroup because if two points have real coordinates, then so do their sum and difference. And since we are assuming the coefficients a,b,c are rational numbers, it is even true that the rational points form a subgroup of the group of real points. So we have a big group and some subgroups :

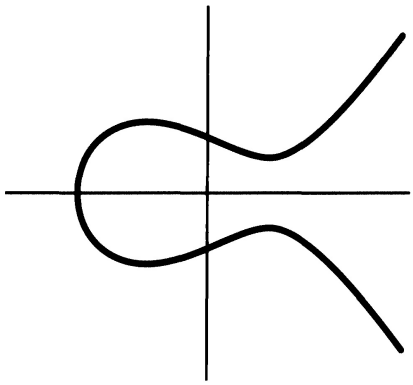
$$\mathcal{O} \subset E(\mathbb{Q}) \subset E(\mathbb{R}) \subset E(\mathbb{C})$$

Definition 2.2.1. *Let $\Lambda \subset \mathbb{C}$ be a lattice, that is, Λ is a discrete subgroup of $\mathbb{C}$ that contains an $\mathbb{R}$-basis for $\mathbb{C}$*

An elliptic function (relative to the lattice Λ) is a meromorphic function $f(z)$ on $\mathbb{C}$ that satisfies

$$f(z + w) = f(z) \qquad \forall z \in \mathbb{C} \text{ and } \qquad \forall w \in \Lambda$$

The set of all such functions is denoted by $\mathbb{C}(\Lambda)$. It is clear that $\mathbb{C}(\Lambda)$ is a field.



A Cubic Curve with One Real Component

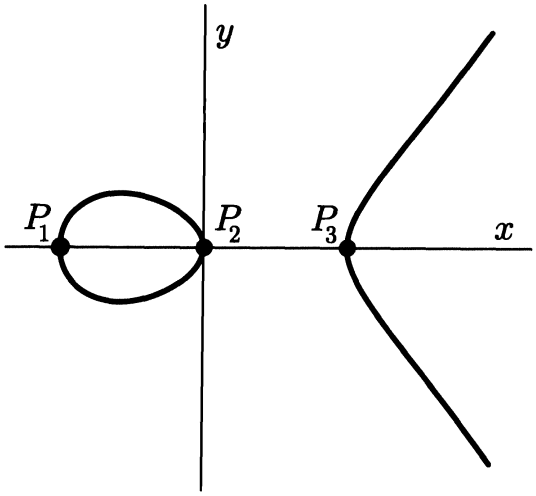


Figure 2.1: A Cubic Curve with Two Real Components

Remark 2.2.2. *A holomorphic elliptic function, i.e., an elliptic function with no poles, is constant. Similarly, an elliptic function with no zeros is constant.*

Definition 2.2.3. *Let $\Lambda \subset \mathbb{C}$ be a lattice. The Weierstrass $\wp$-function (relative to Λ) is defined by the series*

$$\wp(z;\Lambda) = \frac{1}{z^2} + \sum_{w\in\Lambda, w\neq=0} \left\{ \frac{1}{(z-w)^2} - \frac{1}{w^2} \right\}$$

The Eisenstein series of weight $2k(\Lambda)$ is the series

$$G_{2k}(\Lambda) = \sum_{w\in\Lambda, w\neq 0} w^{-2k}$$

Proposition 2.2.4. *The series defining the Weierstrass $\wp$-function converges absolutely and uniformly on every compact subset of $\mathbb{C}(\Lambda)$. The series defines a meromorphic function on $\mathbb{C}$ having a double pole with residue 0 at each lattice point and no other poles .*

Proposition 2.2.5. *A holomorphic elliptic function, i.e., an elliptic function with no poles, is constant*

Theorem 2.2.6. (a) *The Laurent series for $\wp(z)$ around $z = 0$ is given by*

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

(b) *For all $z \in \mathbb{C}\ \Lambda$, the Weierstrass $\wp$-function and its derivative satisfy the relation*

$$\wp'(z)^2 = 4\wp(z)^3 - 60G_4\wp(z) - 140G_6$$

Proof. **(a)** For all z with $|z| < |w|$ we have

$$\frac{1}{(z-w)^2} - \frac{1}{w^2} = \frac{1}{w^2}\left(\frac{1}{(1-z/w)^2} - 1\right) = \sum_{n=1}^{\infty}(n+1)\frac{z^n}{w^{n+2}}$$

Substituting this formula into the series for $\wp(z)$ and reserving the order of summation gives the desired result.

(b) We write out the first few terms of various Laurent expansions :

$$\begin{aligned}
\wp(z) &= z^{-2} + 3G_4 z^2 + 7G_8 z^6 + 9G_{10} z^8 + 11G_{12} z^{10} + 13G_{14} z^{12} + \dots) \\
\wp(z)^2 &= (z^{-2} + 3G_4 z^2 + 7G_8 z^6 + 9G_1 0 z^8 + 11G_{12} z^{10} + 13G_{14} z^{12} + \dots) \\
&\quad (z^{-2} + 3G_4 z^2 + 7G_8 z^6 + 9G_1 0 z^8 + 11G_1 2 z^{10} + 13G_{14} z^{12} + \dots) \\
\wp(z)^2 &= z^{-4} + 6G_4 + z^2(5G_6 + 5G_6) + z^4(7G_8 + 9G_4^2 + 7G_8) + z^6(9G_{10} + \\
&\quad 15G_4 G_6 + 9G_{10}) + z^8(11G_{12} + 21G_4 G_8 + 25G_6^2 + 21G_4 G_8 + 11G_{12}) + \dots \\
\wp(z)^3 &= (z^{-2} + 3G_4 z^2 + 7G_8 z^6 + 9G_{10} z^8 + 11G_{12} z^{10} + 13G_{14} z^{12} + \dots) \\
&\quad (z^{-4} + 6G_4 + z^2(5G_6 + 5G_6) + z^4(7G_8 + 9G_4^2 + 7G_8) + z^6(9G_{10} \\
&\quad + 15G_4 G_6 + 9G_{10}) + z^8(11G_{12} + 21G_4 G_8 + 25G_6^2 + 21G_4 G_8 + 11G_{12}) + \dots) \\
\wp(z)^3 &= z^{-6} + z^{-2}(6G_4 + 3G_4) + (10G_6 + 5G - 6) + z^2(14G_8 + 9G_4^2 + 18G_4^2) + \\
&\quad z^4(18G_{10} + 15G_4 G_6 + 30G_4 G_6) + z^6(22G_{12} + 42G_4 G_8 + 25G_6^2 + \\
&\quad 42G_4 G_8 + 27G_4^3 + 50G_6^2 + 42G_4 G_8 + 11G_{12}) + \dots \\
\wp(z)' &= -2z^{-3} + 6G_4 z + 20G_6 z^3 + 42G_8 z^5 + 72G_{10} z^7 + 110G_{12} z^9 + \dots \\
\wp(z)'^2 &= (-2z^{-3} + 6G_4 z + 20G_6 z^3 + 42G_8 z^5 + 72G_{10} z^7 + 110G_{12} z^9 + \dots) \\
&\quad (-2z^{-3} + 6G_4 z + 20G_6 z^3 + 42G_8 z^5 + 72G_{10} z^7 + 110G_{12} z^9 + \dots) \\
&= 4z^{-6} + z^{-2}(-12G_4 - 12G_4) + (-40G_6 - 40G_6) + z^2(-84G_8 + 36G_4^2 \\
&\quad - 84G_8) + z^4(-144G_{10} + 120G_4 G_6 + 120G_4 G_6 - 144G_{10}) + \\
&\quad z^6(-220G_{12} + 252G_4 G_8 + 400G_6^2 + 252G_4 G_8 - 220G_{12}) + \dots \\
\wp(z)'^2 &= 4z^{-6} + z^{-2}(-24G_4) - 80G_6 + z^2(-168G_8 + 36G_4^2) + \\
f(z) &= \wp(z)'^2 - 4\wp(z)^3 + 60G_4 \wp(z) + 140G_6 \\
&= \{4z^{-6} + z^{-2}(-24G_4) - 80G_6 + z^2(-168G_8 + 36G_4^2) + \\
&\quad z^4(240G_4 G_8 - 288G_{10}) + z^6(-440G_{12} + 504G_4 G_8 + 400G_6^2) + \dots\} \\
&\quad - 4\{z^{-6} + z^{-2}(6G_4 + 3G_4) + (10G_6 + 5G - 6) + z^2(14G_8 + 9G_4^2 + 18G_4^2) \\
&\quad + z^4(18G_{10} + 15G_4 G_6 + 30G_4 G_6) + z^6(22G_{12} + 42G_4 G_8 + 25G_6^2 + 42G_4 G_8 \\
&\quad + 27G_4^3 + 50G_6^2 + 42G_4 G_8 + 11G_{12}) + \dots\} + 60G_4\{z^{-2} + 3G_4 z^2 + \\
&\quad 7G_8 z^6 + 9G_{10} z^8 + 11G_{12} z^{10} + 13G_{14} z^{12} + \dots)\} + 140G_6 \\
&= z^2(-168G_8 + 36G_4^2 - 56G_8 - 108G_4^2 + 180G_4^2) + z^4(240G_4 G_6 - 288G_{10} - 72G_{10} \\
&\quad - 180G_4 G_6) + z^6(-440G_{12} + 504G_4 G_8 + 400G_6^2 - 132G_{12} - 504G_4 G_8 \\
&\quad - 300G_6^2 - 108G_4^3 + 420G_4 G_8) + \dots \\
&= z^2(-224G_8 + 108G_4^2) + z^4(60G_4 G_6 - 360G_{10}) + z^6(-572G_{12} + 420G_4 G_8 \\
&\quad + 100G_6^2 - 108G_4^3) + \dots
\end{aligned}$$

$f(z)$is holomorphic at $z = 0$ and satisfies $f(0) = 0$. But $f(z)$ is an elliptic function relative to Λ, and from above proposition it is holomorphic away from Λ, so $f(z)$ is a holomorphic elliptic function. Then above proposition says that $f(z)$ is constant, and the fact that $f(0) = 0$ implies that f is identically zero.

□

So we have proved that Weierstrass $\wp(u)$ satisfies the defferential equation

$$(\wp')^2 = 4\wp^3 - g_2\wp - g_3, \qquad \text{where } \wp' = \frac{d\wp}{du},\ g_2 = 60G_4,\ g_3 = 140G_6$$

Thus for every complex number u we get a point

$$P(u) = (\wp(u), (\wp'(u) \tag{2.1}$$

on the given curve, in general a point with complex coordinates. So we obtain a map from the complex u plane to $E(\mathbb{C})$ and we send the points in Λ, which are the poles of $\wp$, to $\mathcal{O}$.

Proposition 2.2.7. *[Kob, Prop. 10] The map given by 2.1 is one to one correspondence between $\mathbb{C}/\Lambda$ and the elliptic curve $y^2 = x^3 - g_2x - g_3$ in $\mathbb{P}^2_{\mathbb{C}}$.*

2.3 Discriminant

Our goal in this chapter is to prove Nagell-Lutz theorem which says that every torsion element of $E(\mathbb{Q})$ must have integer co-ordinate, and either $y = 0$ or $y|$discriminant.let us recall the notion of discriminant. Suppose $E : y^2 = x^3 + ax^2 + bx + c$ is rational elliptic curve. Now substitute $x = X/d^2$ and $y = Y/d^3$ then the elliptic curve becomes $Y^2 = X^3 + d^2aX^2 + d^4bX + d^6c$. So by choosing appropriate d we can make d^2a, d^4b and d^6c as integers.
So from now on we will assume that our cubic curve is given by an equation having integer coefficients.
The discriminant of $f(x)$ is the quantity :

$$\triangle = -4a^3 + a^2b^2 + 18abc - 4b^3 - 27c^2$$

if $a = 0$ then $\triangle = -4b^3 - 27c^2$

If we assume $f(x)$ over complex number and $\alpha_1, \alpha_2, \alpha_3$ are the roots of polynomial $f(x)$.
Then we can write $f(x)$ as :

$$f(x) = (x - \alpha_1)(x - \alpha_2)(x - \alpha_3)$$

And we can check that :

$$\triangle = (\alpha_1 - \alpha_2)^2(\alpha_1 - \alpha_3)^2(\alpha_2 - \alpha_3)^2$$

and so the non-vanishing of $\triangle$ tells us that the roots of $f(x)$ are distinct.

we can also express discriminant in terms of coefficients of cubic equation :

$$\begin{aligned}
f(x) &= (x-\alpha_1)(x-\alpha_2)(x-\alpha_3) \\
&= (x-\alpha_2)(x-\alpha_3)+(x-\alpha_1)(x-\alpha_3)+(x-\alpha_1)(x-\alpha_2) \\
\triangle &= (\alpha_1-\alpha_2)^2(\alpha_1-\alpha_3)^2(\alpha_2-\alpha_3)^2 \\
&= (\alpha_1-\alpha_2)(\alpha_1-\alpha_3)(\alpha_1-\alpha_2)(\alpha_2-\alpha_3)(\alpha_1-\alpha_3)(\alpha_2-\alpha_3) \\
&= -(\alpha_1-\alpha_2)(\alpha_1-\alpha_3)-(\alpha_1-\alpha_2)(\alpha_2-\alpha_3)(\alpha_1-\alpha_3)(\alpha_2-\alpha_3) \\
&= -f'(\alpha_1)f'(\alpha_2)f'(\alpha_3) \\
\triangle &= -\prod_{i=1}^{3} f'(\alpha_i)
\end{aligned}$$

Now we will prove one proposition which will be useful for proving Nagell-Lutz theorem.

Proposition 2.3.1. *Suppose $f(x)$ is a polynomial over K. Then there are two polynomials $F(x), G(x) \in K[x]$ such that the discriminant of the polynomial $f(x)$*

$$\triangle = F(x)f(x) + G(x)f'(x)$$

For proving this proposition we have to introduce resultant of two polynomial and following lemma.

Definition 2.3.2. *Let*

$$f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$$

$$g(x) = b_0 + b_1x + b_2x^2 + \cdots + b_mx^m$$

be two polynomial of degree n, m respectively over K. Let $\alpha_i (1 \le i \le n)$ and $\beta_j (1 \le j \le m)$ be roots of $f(x)$ and $g(x)$. The resultant $R(f,g)$ of $f(x)$ and $g(x)$ is defined by

$$R(f,g) = a_n^m b_m^n \prod_{i=1}^{n}\prod_{j=1}^{m}(\alpha_i - \beta_j)$$

If we define $f(x) = a_n \prod_{i=1}^{n}(x-\alpha_i)$ and $g(x) = b_m \prod_{j=1}^{m}(x-\beta_j)$ then

$$R(f,g) = a_n^m \prod_{i,j=1}^{n,m} b_m(\alpha_i - \beta_j) = a_n^m \prod_{i=1}^{n} g(\alpha_i) = (-1)^{nm} b_m^n \prod_{j=1}^{m} f(\beta_j)$$

So from this we can conclude that

$$R(f,f') = a_n^{n-1} \prod_{i=1}^{n} f'(\alpha_i) \tag{2.2}$$

Lemma 2.3.3. *Suppose $f(x)$ and $g(x)$ are polynomials in $K[x]$. Then there are polynomials $F(x)$ and $G(x)$ in $K[x]$, such that*

$$R(f,g) = F(x)f(x) + G(x)g(x)$$

Proof. Let

$$f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n \qquad (a_n \neq 0)$$

$$g(x) = b_0 + b_1x + b_2x^2 + \cdots + b_mx^m \qquad (b_m \neq 0)$$

be two polynomial of degree n, m respectively over K.
If $R(f,g) = 0$, there is nothing to prove. So let $R(f,g) = d \neq 0$

Consider the system of equations

$$x^i f(x) = a_0 x^i a_1 x^{i+1} + \cdots + a_n x^{i+n} \qquad (i = 0, 1, \ldots, m-1)$$

$$x^j g(x) = b_0 + b_1 x^{j+1} + \cdots + b_m x^{j+m} \qquad (j = 0, 1, \ldots, n-1).$$

These equation can be rewritten as a single matrix equation $AX = Y$, where

$$A = \begin{pmatrix} a_0 & a_1 & \ldots & a_n & \\ & a_0 & \ldots & & a_n \\ & & \cdots & & \\ b_0 & b_1 & \ldots & b_n & \\ & b_0 & \ldots & & b_m \\ & & & \cdots & \end{pmatrix}, \qquad X = \begin{pmatrix} 1 \\ x \\ x^2 \\ \vdots \\ x^{m+n-1} \end{pmatrix}, \qquad Y = \begin{pmatrix} f(x) \\ f(x)x \\ \vdots \\ g(x) \\ g(x)x \\ \vdots \\ g(x)x^{n-1} \end{pmatrix}$$

The missing entries A are all zeros.By the definition of resultant $R(f, g) = \det(A) = d \neq 0$.
Since $d \neq 0, A^{-1} = (1/d)adj(A)$, where the matrix $adj(A) = (A_{ij})$ consists of the cofactors A_{ij} of A . Obviously, $X = (1/d)(adjA)Y$. Solving for the first coordinate of X, we obtain

$$d = \Big(\sum_{j=1}^{m} A_{1j} x^{j-1}\Big) f(x) + \Big(\sum_{j=m+1}^{m+n} A_{1j} x^{j-m-1}\Big) g(x)$$

Put

$$F(x) = \sum_{j=1}^{m} A_{1j} x^{j-1} \qquad \text{and} \qquad G(x) = \sum_{j=m+1}^{m+n} A_{1j} x^{j-m-1}$$

We get

$$R(f, g) = F(x)f(x) + G(x)g(x)$$

□

Proof of lemma *2.3.1.* For proving this lemma first we claim that :

$$\triangle = (-1)^{n(n-1)/2} \frac{1}{a_n} R(f, f') \qquad (a)$$

For proving this claim we will prove that

$$\triangle = a_n^{2n-2} \{(-1)^{-\frac{n(n-1)}{2}} a_n^{-n}\} \prod_{i=1}^{n} f'(\alpha_i)$$

Let $f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 + a_0$ be a polynomial of degree $n \in K[X], Kisfield.$ If $\alpha_1, \alpha_2, \ldots, \alpha_n$

are the roots of the polynomial and $N = 1, 2, 3, \ldots, n$.

$$
\begin{aligned}
f(x) &= a_n(x-\alpha_1)(x-\alpha_2)(x-\alpha_3)\ldots(x-\alpha_n) \\
f'(x) &= a_n\{(x-\alpha_2)(x-\alpha_3)\ldots(x-\alpha_n) + (x-\alpha_1)(x-\alpha_3)\ldots(x-\alpha_n) \\
&\quad + (x-\alpha_1)(x-\alpha_2)(x-\alpha_4)\ldots(x-\alpha_n) + \cdots + (x-\alpha_1)(x-\alpha_2) \\
&\quad \ldots(x-\alpha_{n-1})\} \\
f'(x) &= a_n\left\{\prod_{1\neq i\in N}(x-\alpha_i) + \prod_{1\neq i\in N}(x-\alpha_i) + \cdots + \prod_{1\neq i\in N}(x-\alpha_i)\right\} \\
\Rightarrow f'(\alpha_1) &= a_n \prod_{1\neq i\in N}(\alpha_1-\alpha_i) \\
&= (-1)^0 a_n(\alpha_1-\alpha_2)(\alpha_1-\alpha_3)\ldots(\alpha_1-\alpha_n) \\
f'(\alpha_2) &= a_n(\alpha_2-\alpha_1)(\alpha_2-\alpha_3)\ldots(\alpha_2-\alpha_n) \\
&= (-1)^1 a_n(\alpha_1-\alpha_2)(\alpha_2-\alpha_3)\ldots(\alpha_1-\alpha_n) \\
f'(\alpha_3) &= a_n(\alpha_3-\alpha_1)(\alpha_3-\alpha_2)(\alpha_3-\alpha_4)\ldots(\alpha_3-\alpha_n) \\
&= (-1)^2 a_n(\alpha_1-\alpha_3)(\alpha_2-\alpha_3)(\alpha_3-\alpha_4)\ldots(\alpha_3-\alpha_n) \\
f'(\alpha_4) &= a_n(\alpha_4-\alpha_1)(\alpha_4-\alpha_2)(\alpha_4-\alpha_3)(\alpha_4-\alpha_5)\ldots(\alpha_4-\alpha_n) \\
&= (-1)^3 a_n(\alpha_1-\alpha_4)(\alpha_2-\alpha_4)(\alpha_3-\alpha_4)(\alpha_4-\alpha_5)\ldots(\alpha_4-\alpha_n) \\
&\quad \vdots \qquad\qquad \vdots \\
&\quad \vdots \qquad\qquad \vdots \\
f'(\alpha_{n-1}) &= (-1)^{n-2} a_n(\alpha_1-\alpha_{n-1})(\alpha_2-\alpha_{n-1})\ldots(\alpha_{n-2}-\alpha_{n-1})(\alpha_{n-1}-\alpha_n) \\
f'(\alpha_n) &= (-1)^{n-1} a_n(\alpha_1-\alpha_n)(\alpha_2-\alpha_{n-1})(\alpha_3-\alpha_{n-1})\ldots(\alpha_{n-1}-\alpha_n) \\
\Rightarrow \prod_{i=1}^{n} f'(\alpha_i) &= (-1)^{\{1+2+3+\cdots+(n-1)\}} a_n^n \prod_{1\leq i<j\leq n}(\alpha_i-\alpha_j)^2 \\
\prod_{i=1}^{n} f'(\alpha_i) &= (-1)^{\frac{n(n-1)}{2}} a_n^n \prod_{1\leq i<j\leq n}(\alpha_i-\alpha_j)^2 \\
\Rightarrow \prod_{1\leq i<j\leq n}(\alpha_i-\alpha_j)^2 &= (-1)^{-\frac{n(n-1)}{2}} a_n^{-n} \prod_{i=1}^{n} f'(\alpha_i)
\end{aligned}
$$

We know by the definition of discriminant of n degree polynomial that :

$$\triangle = a_n^{2n-2} \prod_{1\leq i<j\leq n}(\alpha_i-\alpha_j)^2$$

Substitute the value of

$$\prod_{1\leq i<j\leq n}(\alpha_i-\alpha_j)^2$$

in the definition of discriminant then we get :

$$\triangle = a_n^{2n-2}\{(-1)^{-\frac{n(n-1)}{2}} a_n^{-n}\} \prod_{i=1}^{n} f'(\alpha_i)$$

$$\triangle = \{(-1)^{-\frac{n(n-1)}{2}} a_n^{n-2}\} \prod_{i=1}^{n} f'(\alpha_i) \tag{2.3}$$

and also from the equation 2.2 we have that

$$R(f, f') = a_n^{n-1} \prod_{i=1}^{n} f'(\alpha_i)$$

$\Rightarrow \prod_{i=1}^{n} f'(\alpha_i) = a_n^{-n+1} R(f, f')$. Now substitute the value of $\prod_{i=1}^{n} f'(\alpha_i)$ in the above equation $\triangle = a_n^{2n-2}\{(-1)^{-\frac{n(n-1)}{2}} a_n^{-n}\} \prod_{i=1}^{n}$ we get :

$$\triangle = (-1)^{n(n-1)/2} \frac{1}{a_n} R(f, f') \qquad (a)$$

We know from the lemma 2.3.3 that

$$R(f, f') = F'(x)f(x) + G'(x)f'(x)$$

for some polynomial $F'(x)$ and $G'(x)$ in $K[x]$.So On substituting

$$F(x) = (-1)^{n(n-1)/2} \frac{1}{a_n} F'(x) \text{ and } G(x) = (-1)^{n(n-1)/2} \frac{1}{a_n} G'(x)$$

in the above expression (a) we get desired result:

$$\triangle = F(x)f(x) + G(x)f'(x)$$

□

Example 2.3.4. *For cubic curves : $y^2 = x^3 + 4$, determine all of the rational points of finite order.*

Solution $E : y^2 = x^3 + 4$
Comparing this curve with $C : y^2 = x^3 + ax^2 + bx + c$.Then we get

$$a = 0, \qquad b = 0, \qquad c = 4, \qquad \triangle = -27c^2 = 432$$

Possible y values $\in \{0, \pm1, \pm2, \pm3, \pm4, \pm6, \pm12\}$
If $y = 0$ then $x^3 + 4 = 0 \Longrightarrow x \notin \mathbb{Z}$ so there is no point with $y = 0$
If $y = \pm1$ then $x^3 + 4 = 1 \Longrightarrow x^3 = -3 \Longrightarrow x \notin \mathbb{Z}$ so there is no point with $y = \pm1$
If $y = \pm2$ then $x^3 + 4 = 4 \Longrightarrow x^3 = 0 \Longrightarrow x = 0 \in \mathbb{Z}$ so there are two points $(0, 2)$ and $(0, -2)$ with $y = \pm2$
If $y = \pm3$ then $x^3 + 4 = 9 \Longrightarrow x^3 = 5 \Longrightarrow x \notin \mathbb{Z}$ so there is no point with $y = \pm3$
If $y = \pm4$ then $x^3 + 4 = 16 \Longrightarrow x^3 = 12 \Longrightarrow x \notin \mathbb{Z}$ so there is no point with $y = \pm4$
If $y = \pm6$ then $x^3 + 4 = 36 \Longrightarrow x^3 = 32 \Longrightarrow x \notin \mathbb{Z}$ so there is no point with $y = \pm6$
If $y = \pm12$ then $x^3 + 4 = 144 \Longrightarrow x^3 = 140 \Longrightarrow x \notin \mathbb{Z}$ so there is no point with $y = \pm12$
So all possible points are as follows :
$(0, 2), \qquad (0, -2) \qquad$ and $\mathcal{O}$
Moreover by duplication formula we get :
$(0, 2) + (0, 2) = (0, -2) \Longrightarrow 2(0, 2) = (0, -2) \Longrightarrow$ order of $(0, 2) = 3$
$(0, -2) + (0, -2) = (0, 2) \Longrightarrow 2(0, -2) = (0, 2) \Longrightarrow$ order of $(0, -2) = 3$
And order of $\mathcal{O} = 1$

2.4 Nagell-Lutz theorem

Theorem 2.4.1 (Nagell-Lutz)**.** *Let*

$$y^2 = f(x) = x^3 + ax^2 + bx + c$$

be non-singular cubic curve with $a, b, c \in \mathbb{Z}$ and let $\triangle$ be the discriminant of the cubic polynomial $f(x)$. Let $P = (x, y)$ be a rational point of finite order. Then x and y are integer; and either $y = 0$, in which case P has order 2, or else y divides $\triangle$.There is a finite number of such points.

Firstly we will introduce some definitions,lemmas and proposition for proving Nagell-Lutz theorem.

Remark 2.4.2. *An useful observation for our proof is that any rational number can be expressed by the following formula :*

$$\frac{m}{n}p^v$$

where the prime number p does not divide either m or n, where $n > 0$, and where v is some integer. We define the order of a rational number to be the integer v :

$$\mathrm{ord}\Big(\frac{m}{n}p^v\Big) = v$$

Lemma 2.4.3. *Fix a prime p. For any point $(x, y) \in E(\mathbb{Q})$, if p divides the denominator of x, then p divides the denominator of y.*

Proof. Consider a point $(x, y) \in E(\mathbb{Q})$, where there exists a prime p dividing the denominator of x. Because x and y are rational numbers, we can express them as follows :

$$x = \frac{m}{np^\mu} \qquad y = \frac{u}{wp^\sigma}$$

Because p divides the denominator of x, we have that $\mu > 0$. This proof, then, aims to show that $\sigma > 0$. By construction, we also know that $p \nmid m, n, u, w$. By substituting our equations for x and y into the equation $y^2 = x^3 + ax^2 + bx + c$, we get :

$$\frac{u^2}{w^2 p^{2\sigma}} = \frac{m^3}{n^3 p^{3\mu}} + \frac{am^2}{n^2 p^{2\mu}} + \frac{bm}{np^{\mu}} + c$$

Finding a common denominator, this becomes :

$$\frac{u^2}{w^2 p^{2\sigma}} = \frac{m^3 + am^2 np^{\mu} + bmn^2 p^{2\mu + cn^3 p^{3\mu}}}{n^3 p^{3\mu}}$$

We can now examine the orders of both sides of this equation. Because $p \nmid u^2$ and $p \nmid w^2$, we have :

$$\mathrm{ord}\Big(\frac{u^2}{w^2 p^{2\sigma}}\Big) = \mathrm{ord}\Big(\frac{u^2}{w^2} p^{-2\sigma}\Big) = -2\sigma$$

For the right side of the equation, we know that $p \nmid n$ and thus that $p \nmid n^3$. We also know that$p \nmid m$, so it is true that $p \nmid (m^3 + am^2 np^{\mu} + bmn^2 p^{2\mu} + cn^3 p^{3\mu})$. Thus, we have :

$$\mathrm{ord}\Big(\frac{m^3 + am^2 np^{\mu} + bmn^2 p^{2\mu + cn^3 p^{3\mu}}}{n^3 p^{3\mu}}\Big) = -3\mu$$

Because both sides of our equation must have the same order, these two results give us that $2\sigma = 3\mu$ In particular, $\sigma > 0$, and so p divides the denominator of y. Further, the relation $2\sigma = 3\mu$ means that $2|\mu$ and $3|\sigma$, so we have $\mu = 2v$ and $\sigma = 3v$ for some integer $v > 0$.

Similarly, if we assume that p divides the denominator of y, we find by the same calculation that the exact same result holds, namely, $\mu = 2v$ and $\sigma = 3v$ for some integer $v > 0$. Thus, if p appears in the denominator of either x or y, then it is in the denominator of both of them □

Definition 2.4.4. *For an elliptic curve E over $\mathbb{Q}$, we define the set $E(p^v)$ by :*

$$E(p^v) = \{(x, y) \in E(\mathbb{Q}) \qquad |\mathrm{ord}(x) \leq -2v \text{ and } \mathrm{ord}(y) \leq -3v\}$$

Intuitively, $E(p^v)$ is the set of all points of $E(\mathbb{Q})$ in which the denominators of the coordinates of x and y are divisible by powers of p greater than $2v$ and $3v$, respectively. By convention, we also include the point at infinity,$\mathcal{O}$, in all sets $E(p^v)$.

Additionally, it is intuitively clear that $E(\mathbb{Q}) \supset E(p) \supset E(p^2) \supset E(p^3) \supset \dots$, from the definition of the sets $E(p^v)$.

Lemma 2.4.5. *$E(p^v)$ is a subgroup of $E(\mathbb{Q})$ for all v.*

Proof. We will define two new variables t and s by

$$t = \frac{x}{y} \qquad\qquad s = \frac{1}{y}$$

Substituting in t and s, our equation for the elliptic curve ($y^2 = x^3 + ax^2 + bx + c$) becomes :

$$s = t^3 + at^2 s + bts^2 + cs^3$$

Every point (x, y) on E has a unique corresponding point on the graph defined by Equation Notably, this is with the exception of points of order 2 on E, because these points have $y = 0$ and therefore make s undefined. However, the point at infinity $\mathcal{O}$ is expressed by a point on the graph of Equation namely, the point $(0, 0)$. Following figure 2.2 shows both graphs in this mapping. Similarly, lines passing through E in

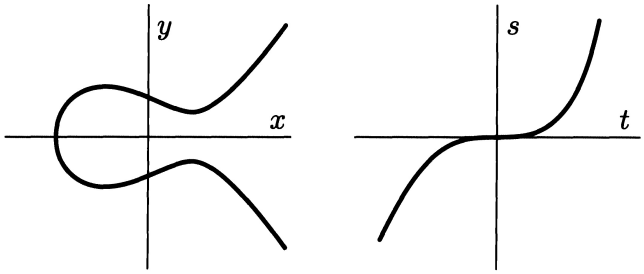


Figure 2.2:

the (x, y) plane have corresponding lines in the (t, s) plane. If the equation for a line in the (x, y) plane is $y = \lambda x + v$, then dividing the equation by vy gives us an equation for the corresponding line in the (t, s) plane :

$$\frac{1}{v} = \frac{\lambda}{v}\frac{x}{y} + \frac{1}{y} \Rightarrow s = -\frac{\lambda}{v}t + \frac{1}{v}$$

For adding two points P_1 and P_2 on elliptic curve in $t-s$ plane we connect two points P_1 and P_2 on the curve with a line, and find the third point of intersection (t_3, s_3). In our relation, $\mathcal{O}$ is mapped to $(0, 0)$, so all we have to do is draw a line through (t_3, s_3) and the origin, and find the third point of intersection. Because Equation is an odd function, this just means that $P_3 = (-t_3, -s_3)$. We can find a general formula for this addition. Then, by considering only points in $E(p^v)$, we can show that this way of defining addition makes $E(p^v)$ a group. We will define the ring R_p as the set of all rational numbers such that p does not divide the denominator. Notationally, this means that for all $x \in R_p$, we have that $\text{ord}(x) \geq 0$. The invertible elements of R_p (that is, all elements u that have an inverse v under multiplication in R_p) are called the units of R_p, and are in this case those elements with order equal to 0, or those in which both the numerator and denominator are co-prime to p.

Let (x, y) be a point with rational coordinates in $E(p^v)$. By definition, we have that $\text{ord}(x) \leq -2v$ and $\text{ord}(y) \leq -3v$, so we can express x and y by the following equations :

$$x = \frac{m}{np^{2(v+i)}} \qquad \frac{u}{wp^{3(v+i)}}$$

for some $i \geq 0$. Using our equations for t and s, this yields :

$$t = \frac{x}{y} = \frac{mw}{nu}p^{v+i} \qquad s = \frac{1}{y} = \frac{w}{u}p^{3(v+i)}$$

Thus, for a point to satisfy $(x, y) \in E(p^v), p^v$ must divide the numerator of t, and p^3v must divide the numerator of s, for the associated pair (t, s). This is equivalent to saying that (t, s) must satisfy $t \in p^v R_p$ and $s \in p^{3v} R_p$. So, to show that $E(p^v)$ is a subgroup, then we can simply show that if an arbitrary power of p divides the t coordinate of two points P_1 and P_2, then the same power of p will divide the t coordinate of their sum.

Let $P_1 = (t_1, s_1)$ and $P_2 = (t_2, s_2)$ be distinct points on the curve. There are two possible cases to consider :
(1) $t_1 = t_2$ If $t_1 = t_2$, then $P_1 = -P_2$ by the addition law, so $P_1 + P_2$ must be an element of $E(p^v)$, because they add to the point $(0, 0)$.
(2) $t_1 \neq t_2$ Let $s = \alpha t + \beta$ be the line passing through P_1 and P_2.The slope of the line,α,is given by $\alpha = \frac{s_2 - s_1}{t_2 - t_1}$.We also know that (t_1, s_1) and (t_2, s_2) satisfy the equation $s = t^3 + at^2 s + bts^2 + cs^3$. So, we can attempt to express the slope as a function of the coordinates of P_1 and P_2, as well as the coefficients $a, b,$

and c may subtract the equation forP_1 from the equation for P_2 :

$$s_2 - s_1 = t_2^3 - t_1^3 + a(t_2^2 s_2 - t_1^2 s_1) + b(t_2 s_2^2 - t_1 s_1^2) + c(s_2^3 - s_1^3)$$

This can be reformulated to include factors in the form of $(t_2 - t_1)$ and $(s_2 - s_1)$:

$$s_2 - s_1 = t_2^3 - t_1^3 + a(t_2^2 - t_1^2)s_2 + at_1^2(s_2 - s_1) + b(t_2 - t_1)s_2^2 + bt_1(s_2^2 - s_1^2) + c(s_2^3 - s_1^3)$$

So, factoring out the quantity $(t_2 - t_1)$, we can find an equation for $(t_2 - t_1)$: after some algebra, the result is :

$$\alpha = \frac{s_2 - s_1}{t_2 - t_1} = \frac{t_2^2 + t_1 t_2 + t_1^2 + a(t_2 + t_1)s_2 + bs_2^2}{1 - at_1^2 - bt_1(s_2 + s_1) - c(s_2^2 + s_1 s_2 + s_1^2)}$$

We will put this result aside for now. Next, we will look at addition on the cubic curve. Let $P_3 = (t_3, s_3)$ be the third point of intersection of the line $s = \alpha t + \beta$

, which is drawn through P_1 and P_2, and the cubic curve $s = t^3 + at^2 s + bts^2 + cs^3$ on which P_1 and P_2 lie. The equation with t_1, t_2 and t_3 as roots can be found by substituting the equation of the line $s = \alpha t + \beta$

:

$$\alpha t + \beta = t^3 + at^2(\alpha t + \beta) + bt(\alpha t + \beta)^3$$

Expanding, multiplying, and factoring out powers of t gives us :

$$(1 + a\alpha + \alpha^2 b + c\alpha^3)t^3 + (a\beta + 2b\alpha\beta + 3c\alpha^2\beta)t^2 + (b\beta^2 + 3c\alpha\beta^2 - \alpha)t + c\beta^3 - \beta = 0$$

It is generally true that the sum of the roots of a cubic equation of the form $0 = ax^3 + bx^2 + cx + d$ is equal to $\frac{-b}{a}$.This convenient fact gives us an equation for the sum $t_1 + t_2 + t_3$, based solely upon the coefficients of t^3 and t^2 in the above equation.

$$t_1 + t_2 + t_3 = \frac{a\beta + 2b\alpha\beta + 3c\alpha^2\beta}{1 + a\alpha + \alpha^2 b + c\alpha^3}$$

This is a powerful result that gives us a way to calculate t_3 given only t_1 and t_2, and therefore allows us to find $P_1 + P_2$ for any P_1, P_2 on the curve. We can finally begin to analyze all of the above preliminary results. First,we will look at our extended formula for,given by Equation :

$$\alpha = \frac{s_2 - s_1}{t_2 - t_1} = \frac{t_2^2 + t_1 t_2 + t_1^2 + a(t_2 + t_1)s_2 + bs_2^2}{1 - at_1^2 - bt_1(s_2 + s_1) - c(s_2^2 + s_1 s_2 + s_1^2)}$$

By definition, we know that t_1, t_2, s_1, s_2 are all elements of $p^v R_p$. The formula for the numerator, $\{t_2^2 + t_1 t_2 + t_1^2 + a(t_2 + t_1)s_2 + bs_2^2\}$, when expanded out, satisfies the condition that every term includes two of the elements t_1, t_2, s_1, s_2 multiplied together. Thus, $p^2 v$ divides the numerator of α, and it is therefore an element of $p^2 v R_p$. The denominator of α is $\{1 - at_1^2 - bt_1(s_2 + s_1) - c(s_2^2 + s_1 s_2 + s_1^2)\}$, in which all terms except for 1 are divisible by $p^2 v$ by a similar argument. Because of the value 1, the denominator is co-prime to p, and is therefore a unit in R_p. So, looking at α in its entirety, we have that $p^2 v$ divides the numerator and not the denominator, giving us the result that $\alpha \in p^{2v} R_p$.

From our equation for the line through P_1 and P_2, we know that $s_1 = \alpha t_1 + \beta$.Because $s_1 \in p^v R_p$, we know that $s_1 \in p^{3v} R_p$. And, because $\alpha \in p^{2v} R_p$ and $t_1 \in p^v R_p$, we have that $t_1 \in p^{3v} R_p$. Therefore, the equation for the line gives us that $\beta \in p^{3v} R_p$. Finally, we can analyze Equation

$$t_1 + t_2 + t_3 = \frac{a\beta + 2b\alpha\beta + 3c\alpha^2\beta}{1 + a\alpha + \alpha^2 b + c\alpha^3}$$

through a process similar to our analysis of α . Similarly to the denominator of α, the denominator of the

equation for $t_1 + t_2 + t_3$ is a unit in R_p.The term $\alpha\beta$ in the numerator of Equation

$$t_1 + t_2 + t_3 = \frac{a\beta + 2b\alpha\beta + 3c\alpha^2\beta}{1 + a\alpha + \alpha^2 b + c\alpha^3}$$

gives us that $t_1 + t_2 + t_3 \in p^{3v}R_p$. But we know by assumption that t_1 and t_2 are elements of p^vR_p, so t_3 must be an element of p^vR_p as well, implying that $-t_3 \in p_p^v$.

Thus, if the t-coordinates of P_1 and P_2 are in p^vR_p, then the t-coordinate of $P_1 + P_2$ is also in p^vR_p. Also, because the curve is symmetric about the origin, we know that if the t-coordinate of P is in p^vR_p, then the t-coordinate of $-P$ is also in p^vR_p. This shows that $E(p^v)$ is closed under both addition and negatives, making it a subgroup of $E(\mathbb{Q})$.

In proving that $E(p^v)$ is a subgroup of $E(\mathbb{Q})$, we also proved a stronger result : that $t_1+t_2+t_3 \in p^{3v}R_p$. So we know that, for any $P_1, P_2 \in E(p^v)$,

$$t(P_1) + t(P_2) - t(P_1 + P_2) \in p^{3v}R_p;$$

where $t(P_1)$ denotes the t-coordinate of the (t, s) pair associated with P. So, the numerator of the sum of t_1, t_2 and $-t_3$ must be divisible by p^{3v}. This lends itself to a useful reformulation :

$$t(P_1 + P_2) \equiv t(P_1) + t(P_2) \qquad \mod p^{3v}R_p$$

We can use this fact to finally prove that points of finite order on $E(\mathbb{Q})$ have integer coordinates. □

Lemma 2.4.6. *Given an elliptic curve E, for all prime numbers p, the group $E(p)$ contains no points of finite order (other than $\mathcal{O}$).*

Proof. Let P be a point of finite order m. Let p be some prime number. Because $P \neq \mathcal{O}$, we know that $m > 1$. We will assume that $P \in E(p)$ and establish a contradiction. It is possible that P is contained in some subgroup $E(p^v)$ of $E(p)$. However, P cannot be contained in all such subgroups, because it is impossible for the denominator of P to be divisible by all arbitrarily large powers of P. Thus, there must be some v such that $P \in E(p^v)$, but $P \notin E(p^{v+1})$. Pick this p. There are two possible cases to consider :

1: $p \nmid m$

from above we know that $t(P1 + P2) \equiv t(P1) + t(P2) \mod p^{3v}R_p$.
Because P is a point of order m, we are adding it to itself m times. So, our congruence becomes :

$$t(mP) \equiv mt(P) \qquad p^{3v}R_p$$

Because $mP = \mathcal{O}$, and because $t(\mathcal{O}) = 0$, this becomes $0 \equiv mt(P) \mod p^{3v}R_p$. We also know that m is co-prime to p, making it a unit in R_p. So, we end up with :

$$0 \equiv t(P) \qquad \mod p^{3v}R_p$$

which imply that$P \in E(p^{3v}R_p)$, contradicting the above assumption that $P \notin E(p^{v+1})$.

2: $p \mid m$

Because p divides m, we have that $m = pn$ for some $n \in \mathbb{Z}$. If we let $P' = nP$, then P' has order p, and is an element of $E(p)$ because $P \in E(p)$ by assumption. Similarly to the first case, this yields that

$$0 \equiv pt(P') \qquad \mod p^{3v}R_p$$

. Dividing out p, we get this ultimate result :

$$0 \equiv t(P') \qquad \mod (p^{3v-1}R_p)$$

This gives us that $P' \in E(p^{3v-1})$, which contradicts the assumption that $P' \notin E(p^{v+1})$ because $3v-1 > v+1$.

Therefore, for all primes p, the group $E(p)$ contains no points of finite order greater than 1 □

Corollary 2.4.7. *All points of finite order on $E(\mathbb{Q})$ have integer coordinates.*

Proof. Let $P = (x, y)$ be a point of finite order on $E(\mathbb{Q})$. We know that $P \notin E(p)$ for all primes p, so the denominator of the coordinates of P are not evenly divided by any primes. By definition, a number that cannot be evenly divided by any prime numbers has to be equal to 1, so the denominators of the coordinates of P are 1, and the coordinates must be integers. □

Lemma 2.4.8. *Let $P = (x, y)$ be a point on our cubic curve such that both P and $2P$ have integer coordinates. Then either $= 0$ or $y|\triangle$.*

Proof. Let $P = (x, y)$ and $2P = (X, Y)$
then by duplication formula we know :

$$X = \lambda^2 - a - 2x, \qquad \text{where } \lambda = \frac{f'(x)}{2y}$$

We assume that $y \neq 0$ and prove that $y|\triangle$. Because $y \neq 0$, we know that $2P \neq \mathcal{O}$.Since x, X and a are all integers, it follows that λ is also an integer. Since $2y$ and $f'(x)$ are integers, we see that $2y|f'(x)$; and, in particular, $y|f'(x)$. But $y^2 = f(x)$, so also $y|f(x)$. Now we use the relation

$$\triangle = r(x)f(x) + s(x)f'(x).$$

The coefficients of r and s are integers, so $r(x)$ and $s(x)$ take on integer values when evaluated at the integer x. It follows that y divides $\triangle$. □

Theorem 2.4.9 (Nagell-Lutz)**.** *Let*

$$y^2 = f(x) = x^3 + ax^2 + bx + c$$

be non-singular cubic curve with integer coefficients a, b, c and let $\triangle$ be the discriminant of the cubic polynomial $f(x)$. Let $P = (x, y)$ be a rational point of finite order. Then x and y are integer; and either $y = 0$, in which case P has order 2, or else y divides $\triangle$. There is a finite number of such points.

Proof. From the lemma 2.4.8 and corollary 2.4.7 we conclude that $P = (x, y)$ be a rational point of finite order. Then x and y are integer; and either $y = 0$, in which case P has order 2, or else y divides $\triangle$ and set of all divisors of discriminant $\triangle$ is finite set such points are finte. □

Chapter 3

The Group of rational points

In this chapter we will prove Mordell's theorem which says that the set of all rational points on elliptic curve ($E(\mathbb{Q})$) is finitely generated group which was our ultimate goal. For proving this theorem we want the notion of height so also we will define this term.

3.1 Heights

Let $x = \frac{m}{n}$ be a rational number written in lowest terms. Then we define the height $H(x)$ to be the maximum of the absolute values of the numerator and the denominator :

$$H(x) = H\Big(\frac{m}{n}\Big) = max\{|m|, |n|\}$$

The height of a rational number is positive.
Finiteness property of the height : The set of all rational numbers whose height is less than some fixed number is a finite set.

Height of rational point of elliptic curve

Let $y^2 = x^3 + ax^2 + bx + c$ be an elliptic curve over $\mathbb{Q}$ and $P \in E(\mathbb{Q})$ then we define the height of P as :

$$H(P) = H(x) = H\Big(\frac{m}{n}\Big) = max\{|m|, |n|\}$$

further we define

$$h(P) = \log H(P)$$

So $h(P)$ is always a non negative real number.

3.2 Mordell's theorem

Theorem 3.2.1 (Mordell's theorem)**.** *Let E be an elliptic curve given by the equation*

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

where $a, b, c \in \mathbb{Q}$. Then the group $E(\mathbb{Q})$ is finitely generated Abelian group.

For proving this theorem we need following theorem and some lemmas.

3.3 Descent Theorem

Let Γ be a commutative group. Suppose that there is a function

$$h : \Gamma \longrightarrow [0, \infty)$$

with the following three properties

(a) for every real number M, the set $\{P \in \Gamma : h(P) \leq M\}$ is finite.

(b) for every $P_0 \in \Gamma$, there is a constant κ_0 so that

$$h(P + P_0) \leq 2h(P) + \kappa \qquad \forall P \in \Gamma.$$

(c) there is a constant κ so that

$$h(2P) \geq 4h(P) - \kappa \qquad \forall P \in \Gamma.$$

suppose further that

(d) the subgroup 2Γ has finite index in Γ.

then Γ is finitely generated.

Proof. let $Q_1, Q_2, \ldots, Q_n$ be representatives for the cosets. This means that for any element $P \in \Gamma$ there is an index i_1, depending on P, such that

$$P - Q_{i_1} \in 2\Gamma$$

$$P - Q_{i_1} = 2P_1 \qquad \text{for some} \qquad P_1 \in \Gamma$$

Now we do the same thing with P_1. Continuing this process, we find we can write

$$\begin{aligned} P_1 - Q_{i_2} &= 2P_2 \\ P_2 - Q_{i_3} &= 2P_3 \\ P_3 - Q_{i_4} &= 2P_4 \\ &\vdots \\ P_{m-1} - Q_{i_m} &= 2P_m \end{aligned}$$

where $Q_{i_1}, Q_{i_2}, \ldots, Q_{i_m}$ are chosen from the coset representatives $Q_1, Q_2, \ldots, Q_m$ and $P_1, P_2,$ $\ldots, P_m$ are elements of Γ.From the first equation we have

$$P = Q_{i_1} + 2P_1$$

Now substitute the second equation $P_1 = Q_{i_2} + 2P_2$ into this to get

$$P_1 = Q_{i_1} + 2Q_{i_2} + 4P_2$$

Continuing in this fashion, we obtain

$$P_1 = Q_{i_1} + 2Q_{i_2} + 4Q_{i_3} + \cdots + 2^{m-1}Q_m + 2^m P_m \qquad (a)$$

After substituting $-Q_i$ in second lemma in place of P_0 then we get a constant κ_i such that

$$h(P - Q_i) \leq 2h(P) + \kappa_i \qquad \forall P \in \Gamma$$

We do this for each $Q_i, 1 \leq i \leq n$. Let κ' be the largest of the $\kappa_i's$. Then

$$h(P - Q_i) \leq 2h(P) + \kappa' \qquad \forall P \in \Gamma \qquad \text{and} \qquad 1 \leq i \leq n$$

Now from lemma (3)lemma

$$\begin{aligned} 4h(P_j) \leq h(2P_j) + \kappa = h(P_{j-1} - Q_{i_j}) + \kappa \leq 2h(P_{j-1}) + \kappa' + \kappa \\ h(P_j) \leq \frac{1}{2}h(P_{j-1}) + \frac{\kappa' + \kappa}{4} \\ = \frac{3}{4}h(P_{j-1}) - \frac{1}{4}(h(P_{j-1}) - (\kappa' + \kappa)) \end{aligned}$$

Prom this we see that if $h(P_{j-1}) \geq \kappa' + \kappa$ then

$$h(P_j) \leq \frac{3}{4}h(P_{j-1})$$

So in the sequence of points $P_1, P_2, P_3, \ldots$, as long as the point P_j satisfies the condition $h(P_j) \geq \kappa' + \kappa$, then the next point in the sequence has much smaller height, namely, $h(P_{j+1}) \leq h(P_j)$. But if we start with a number and keep multiplying it by $3/4$, then it approaches zero. So eventually we will find an index m so that $h(P_m) \leq \kappa + \kappa'$
We have now shown that every element $P \in \Gamma$ be written in the form

$$P_1 = a_1Q_1 + a_2Q_2 + a_3Q_3 + \cdots + a_nQ_n + 2^mR$$

for certain integers $a_1, a_2, a_3, \ldots, a_n$ and some point $R \in \Gamma$ satisfying the inequality $h(R) \leq \kappa + \kappa'$. Hence, the set

$$\{Q_1, Q_2, Q_3, \ldots, Q_n\} \cup \{R \in \Gamma : h(R) \leq \kappa + \kappa'\}$$

generates Γ moreover this set is finite so Γ is finitely generated Abelian group. □

Now we will prove $E(\mathbb{Q})$ satisfies the hypothesis of Descent theorem by following lemmas.

Lemma 3.3.1. *For every real number M , the set*

$$\{P \in E(\mathbb{Q}) : h(P) \leq M\}$$

is finite.

Proof. Points in the set have only finitely many possibilities for their x coordinate; and for each x coordinate, there are only two possibilities for the coordinate. □

Lemma 3.3.2. *Let P_0 be a fixed rational point on E. There is a constant κ_0 depending on P_0 and on a, b, c so that*

$$h(P + P_0) \leq 2h(P) + \kappa_0 \qquad \forall \qquad P \in E(\mathbb{Q}).$$

For proving this lemma we will use following remarks.

Remark 3.3.3. *If $P = (x, y)$ is a rational point on our curve,then x and y have the form*

$$x = \frac{m}{e^2} \qquad \text{and} \qquad y = \frac{n}{e^3}$$

for for integers $m, n,$ with $e > 0$ and $\gcd(m, e) = \gcd(n, e) = 1$.

Proof. Let $x = \frac{m}{M}$ and $y = \frac{n}{N}$ are in lowest terms with $M > 0$ and $N > 0$. Substitute these values of x and y in the elliptic curve $y^2 = x^3 + ax^2 + bx + c$ then we get :

$$\begin{aligned} M^3n^2 &= N^2m^3 + aN^2Mm^2 + bN^2M^2m + cN^2M^3 \\ M^3n^2 &= N^2(m^3 + aMm^2 + bM^2m + cM^3) \end{aligned} \tag{1}$$

From above we get $N^2|M^3n^2$ but $\gcd(n, N) = 1$, so $N^2|M^3$. From equation (1) we get $M(M^2n^2 - aN^2m^2 - bN^2Mm - cN^2M^2) = N^2m^3 \Rightarrow M|N^2m^3$ but $\gcd(M, m) = 1$ so $M|N^2$ so $N^2 = kM$ for some $k \in \mathbb{Z}$ use this one in equation(1) we get : $M^3(n^2 - akm^2 - bkm - cN^2) = N^2m^3 \Rightarrow M^3|N^2m^3 \Rightarrow M^3|N^2$ and $M^2|N^2$ hence $M^3 = N^2$ and $M|N$ so let $N = eM$ for some $e \in \mathbb{Z}$ so

$$e^2 = \frac{N^2}{M^2} = \frac{M^3}{M^2} = M \qquad \text{and} \qquad e^3 = \frac{N^3}{M^3} = \frac{N^3}{N^2} = N$$

therefore

$$x = \frac{m}{e^2} \qquad \text{and} \qquad y = \frac{n}{e^3}$$

□

Remark 3.3.4. *If $P = (x, y) \in E(\mathbb{Q})$, then*

$$|n| \leq KH(P)^{3/2}.$$

Proof. By the remark 3.3.3, we have $x = \frac{m}{e^2}$ and $y = \frac{n}{e^3}$. On substituting these values in the elliptic curve $y^2 = x^3 + ax^2 + bx + c$ then we get :

$$n^2 = m^3 + ae^2m^2 + be^4m + ce^6.$$

Take absolute value both side

$$|n^2| = |m^3 + ae^2m^2 + be^4m + ce^6| \leq |m^3| + |ae^2m^2| + |be^4m| + |ce^6|$$

By the definition of height we know that

$$|m| \leq H(P) \qquad \text{and} \qquad e^2 \leq H(P)$$

On substitute these values in the equation above expression we get :

$$\begin{aligned} |n^2| &\leq H(P)^3 + |a|H(P)^3 + |b|H(P)^3 + |c|H(P)^3 \\ &\leq (1 + |a| + |b| + |c|)H(P)^3 \\ &= \sqrt{K}H(P)^3 \\ \Rightarrow |n| &\leq KH(P)^{3/2} \qquad \text{as required.} \end{aligned}$$

□

Proof of lemma 3.3.2. Let $P = (x, y), P_0 = (x_0, y_0) \in E(\mathbb{Q})$ suppose $P + P_0 = (a, b)$ We know by the duplication formula that

$$\xi = \lambda^2 - a - x - x_0 \qquad \text{where} \qquad \lambda = \frac{y - y_0}{x - x_0}$$

$$\xi = \frac{(y-y_0)^2 - (x-x_0)^2(a+x+x_0)}{(x-x_0)^2}$$
$$\xi = \frac{A'y + B'x^2 + C'x + D}{E'x^2 + F'x + G'} \qquad \text{(since} \qquad y^2 - x^3 = ax^2 + bx + c)$$

on multiplying numerator and denominator by lcm of $A', B', C', D', E', F'$and G' then we get :

$$\xi = \frac{Ay + Bx^2 + Cx + D}{Ex^2 + Fx + G}$$

where $A, B, C, D, E, F, G \in \mathbb{Z}$. Now substitute $x = m/e^2$ and $y = n/e^3$ above then we get :

$$\xi = \frac{An + m^2 + Cme^2 + De^4}{Em^2 + fme^2 + Ge^4}$$

by the definition of height

$$H(P + P_0) = max(|An + m^2 + Cme^2 + De^4|, |Em^2 + fme^2 + Ge^4|)$$

and

$$e \leq H(P)^{\frac{1}{2}}, \qquad m \leq H(P)$$

and also we have proved that $n \leq KH(P)^{\frac{3}{2}}$. Using these inequalities we get :

$$H(P + P_0) = H(\xi) \leq max\{|AK| + |B| + |C| + |D|, |E| + |F| + |G|\}H(P)^2$$

Taking the logarithm of both sides gives

$$h(P + P_0) \leq 2h(P) + \kappa_0$$

where κ_0=log max$\{|AK| + |B| + |C| + |D|, |E| + |F| + |G|\}$ depends only on a, b, c and (x_0, y_0) and does not depend on $P = (x, y)$. As required. □

Proposition 3.3.5. *There is a constant κ, depending on a, b, c,so that*

$$h(2P) \geq 4h(P) - \kappa \qquad \forall\ P \in E(\mathbb{Q})$$

For proving this proposition we need following lemmas.

Lemma 3.3.6. *Let $\phi(X)$ and $\psi(X)$ be polynomials with integer coefficients and no common(complex) roots. Let d be the maximum of the degrees of $\phi(X)$ and $\psi(X)$.*

(a) *There is an integer $R \geq 1$, depending on ϕ and ψ, so that for all rational numbers $\frac{m}{n}$*

$$\gcd\left(n^d\phi\Big(\frac{m}{n}\Big), n^d\psi\Big(\frac{m}{n}\Big)\right) \qquad \textit{divides} \qquad R.$$

(b) *there are constants κ_1 and κ_2, depending on ϕ and ψ, so that for all rational numbers $\frac{m}{n}$ which are not roots of ψ*

$$dh\left(\frac{m}{n}\right) + \kappa_1 \leq h\left(\frac{\phi(m/n)}{\psi(m/n)}\right) \leq dh\left(\frac{m}{n}\right) + \kappa_2$$

Proof. **(a)** First we observe that since ϕ and ψ have degree at most d, the quantities $n^d\phi\Big(\frac{m}{n}\Big)$ and $n^d\psi\Big(\frac{m}{n}\Big)$

are both integers.

$$n^d\phi\Big(\frac{m}{n}\Big) = a_0m^d + a_1m^{d-1}n + \cdots + a_dn^d$$
$$n^d\psi\Big(\frac{m}{n}\Big) = b_0m^en^{d-e} + b_1m^{e-1}n^{d-e+1} + \cdots + b_en^d$$

To each notation ,we will let

$$\phi(m,n) = n^d\phi\Big(\frac{m}{n}\Big) \qquad \text{and} \qquad \psi(m,n) = n^d\psi\Big(\frac{m}{n}\Big)$$

So we need to find an estimate for $\gcd(\phi(m,n), \psi((m,n))$ which does not depend on m or n. Since $\phi(X)$ and $\psi(X)$ have no common roots, they are relatively prime in the Euclidean ring $\mathbb{Q}[X]$ Thus, they generate the unit ideal, so we can find polynomials $F(X)$ and $G(X)$ with rational coefficients satisfying

$$F(X)\phi(X) + G(X)\psi(X) = 1$$

Let A be a large enough integer so that $AF(X)$ and $AG(X)$ have integer coefficients. Further, let D be the maximum of the degrees of F and G. Note that A and D do not depend on m or n. Now multiply both sides n by An^{D+d}. This gives

$$An^DF\Big(\frac{m}{n}\Big)\phi\Big(\frac{m}{n}\Big) + An^DG\Big(\frac{m}{n}\Big)\psi\Big(\frac{m}{n}\Big) = An^{D+d}$$

Let $\gamma = \gamma(m,n)$ be the greatest common divisor of $\phi(m,n)$ and $\psi(m,n))$. We have

$$\Big\{n^DAF\Big(\frac{m}{n}\Big)\Big\}\phi\Big(\frac{m}{n}\Big) + \Big\{n^DAG\Big(\frac{m}{n}\Big)\Big\}\psi\Big(\frac{m}{n}\Big) = An^{D+d}$$

Since the quantities in braces are integers, we see that γ divides An^{D+d}. , it certainly divides

$$An^{D+d-1}\phi(m,n) = Aa_0m^dn^{D+d-1} + Aa_1m^{d-1}n^{D+d} + \cdots + Aa_dn^{D+2d-1}$$

But in the sum, every term after the first one contains An^{D+d} as a factor; and we just proved that γ divides An^{D+d}. It follows that γ also divides the first term $Aa_0m^dn^{D+d-1}$. Thus, γ divides $\gcd(An^{D+d}, Aa_0m^dn^{D+d-1})$; and because m and n are relatively prime, we conclude that γ divides $Aa_0m^dn^{D+d-1}$. Notice we have reduced the power of n at the cost of multiplying by a_0. Now using the fact that γ divides $Aa_0m^dn^{D+d-2}\phi(m,n)$ and repeating the above argument shows that γ divides $Aa_0^2m^dn^{D+d-2}$. The pattern is clear, and eventually we reach the conclusion that γ divides Aa_0^{D+d}, which finishes our proof of (a).

(b) Suppose degree of $\phi = d$ and degree of $\psi = e \le d$ then

$$n^d\phi\left(\frac{m}{n}\right) = a_0m^d + a_1m^{d-1} + \cdots + a_dn^d$$

$$n^d\psi\left(\frac{m}{n}\right) = b_0m^{d-e} + b_1m^{d-e+1} + \cdots + b_en^d$$

denote $n^d\phi\Big(\frac{m}{n}\Big)$ by $\phi(m,n)$ and $n^d\psi\left(\frac{m}{n}\right)$ by $\psi(m,n)$
So we have to find gcd of $\phi(m,n)$ and $\psi(m,n)$ which does not depend on m or n. Let

$$\xi = \frac{\phi(\frac{m}{n})}{\psi(\frac{m}{n})} = \frac{n^d\phi(\frac{m}{n})}{n^d\psi(\frac{m}{n})} = \frac{\phi(m,n)}{\psi(m,n)}$$

from the definition of height of rational point we can write for some $K \geq 1$

$$\begin{aligned} H(\xi) &\geq \frac{1}{K} max\{|\phi(m,n)|, |\psi(m,n)|\} \\ &= \frac{1}{K} max\left\{\left|n^d\phi(\frac{m}{n})\right|, \left|n^d\psi(\frac{m}{n})\right|\right\} \\ &\geq \frac{1}{2K}\left(\left|n^d\phi(\frac{m}{n})\right| + \left|n^d\psi(\frac{m}{n})\right|\right) \\ \frac{H(\xi)}{H(m/n)^d} &\geq \frac{1}{2K}\frac{\left(|n^d\phi(\frac{m}{n})| + |n^d\psi(\frac{m}{n}|\right)}{max\{|m|^d, |n|^d\}} \\ &= \frac{1}{2K}\frac{\left(|\phi(\frac{m}{n})| + |\psi(\frac{m}{n}|\right)}{max\{|m/n|^d, 1\}} \\ &= \frac{p(t)}{2K} \qquad \text{where} \qquad p(t) = \frac{|\phi(t)| + |\psi(t)|}{max\{|t|^d, 1\}} \end{aligned}$$

Since ϕ has degree d and ϕ has degree at most d, we see that p has a non-zero limit as $|t|$ approaches infinity. This limit is either $|a_0|$, if ϕ has degree less than d, or $|a_0| + |b_0|$, if ψ has degree equal to d.
Using this fact in the inequality we derived above ,we find that

$$H(\xi) \geq \frac{C_1}{2R} H\Big(\frac{m}{n}\Big)^d$$

the constant C_1 and R do not depend on m and n ,so taking logarithms gives the desired inequality

$$h(\xi) \geq dh\Big(\frac{m}{n}\Big) - \kappa_1$$

with $\kappa_1 = \log(2R/C_1)$

□

Proof of lemma 3.3.5. From lemma 3.3.1 we can exclude some fixed point for inequality in heights.
Let $P = (x, y)$,and write $2P = (a, b)$.then by duplication formula we get

$$a = \lambda^2 - a - 2x \qquad \text{where} \qquad \lambda = \frac{f'(x)}{2y}$$

Substitute value of λ above we get

$$a = \frac{(f'(x))^2 - (8x + 4a)f(x)}{4f(x)} = \frac{x^4 + \ldots}{4x^3 + \ldots}$$

Thus, a is the quotient of two polynomials in x with integer coefficients. Since the elliptic curve $y^2 = f(x)$ is non-singular by assumption, we know that $f(x)$ and $f'(x)$ have no common (complex) roots. It follows that the polynomials in the numerator and the denominator of a also have no common roots.
Now use the previous remark for the expression of a we conclude

$$h(2P) \geq 4h(P) - \kappa$$

□

Proposition 3.3.7. *The index* $[E(\mathbb{Q}) : 2E(\mathbb{Q})]$ *is finite.*

For proving this proposition we need following lemmas, facts and a little lemma.

Lemma 3.3.8. *Let E and $\bar{E}$ be the elliptic curves given by the equation s*

$$E : y^2 = x^3 + ax^2 + bx + c \qquad \text{and} \qquad \bar{E} : y^2 = x^3 + \bar{a}x^2 + \bar{b}x + \bar{c},$$

where

$$\bar{a} = -2a \qquad \text{and} \qquad \bar{b} = a^2 - 4b$$

Let $T = (0,0) \in E$

(a) *There is homomorphism $\phi : E \to \bar{E}$ defined by*

$$\phi(P) = \begin{cases} \left(\frac{y^2}{x^2}, \frac{y(x^2-b)}{x^2}\right) & \text{if } P = (x,y) \neq \mathcal{O}, T, \\ \mathcal{O}, & \text{if } P = \mathcal{O} \text{ or } P = T. \end{cases}$$

The kernel of ϕ is $\mathcal{O}, T$

(b) *Applying the same process to $\bar{E}$ gives a map $\bar{\phi}\bar{E} \longrightarrow \bar{\bar{E}}$. The curve $\bar{\bar{E}}$ is isomorphic to E via the map $(x,y) \longrightarrow (x/4, y/8)$. There is thus a homomorphism $\psi : \bar{E} \longrightarrow E$ defined by*

$$\psi(\bar{P}) = \begin{cases} \left(\frac{\bar{y}^2}{4\bar{x}^2}, \frac{\bar{y}(\bar{x}^2-\bar{b})}{8\bar{x}^2}\right), & \text{if} \bar{P} = (\bar{x}, \bar{y}) \neq \bar{\mathcal{O}}, \bar{T}, \\ \mathcal{O} & \text{if} \quad \bar{P} = \bar{\mathcal{O}} \text{ or } \bar{P} = \bar{T}. \end{cases}$$

(c) *The composition $\psi o \phi : E \longrightarrow E$ is multiplication by two : $\phi o \psi(P) = 2P$.*

Proof of (a). ϕ **is well defined :**
we just have to check that x and y satisfy the equation of $\bar{E}$, which is easy :

$$\begin{aligned} \bar{x}^3 + a\bar{x}^2 + b\bar{x} &= \bar{x}(\bar{x}^2 - 2a\bar{x} + (a^2 - 4b)) \\ &= \frac{y^2}{x^2}\left(\frac{y^4}{x^4} - 2a\frac{y^2}{x^2} + (a^2 - 4b)\right) \\ &= \frac{y^2}{x^2}\left(\frac{(y^2 - ax^2)^2 - 4bx^4}{x^4}\right) \\ &= \frac{y^2}{x^6}\left((x^3 + bx)^2 - 4bx^4\right) \\ &= \left(\frac{y(x^2-b)^2}{x^2}\right)^2 \\ &= \bar{y}^2 \end{aligned}$$

ϕ **is homomorphism :**
we have to show that $\phi(P_1 + P_2) = \phi(P_1) + \phi(P_2)$
case 1 if $P_1, \text{or} P_2 = \mathcal{O}$ then result is automatically true.
case 2 If one of P_1 or $P_2 = T$ then we have to prove

$$\phi(P + T) = \phi(P)$$

Let $P=(x,y), T=(0,0)$ then

$$\begin{aligned} x(P*T) &= \frac{y^2}{x^2} - a - x \\ &= \frac{y^2 - ax^2 - x^3}{x^2} \\ &= \frac{b}{x} \\ y(P*T) &= \frac{y}{x}\Big(\frac{b}{x}\Big) \\ &= \frac{yb}{x^2} \\ \Rightarrow P+T &= \Big(x(P*T), y(P*T)\Big) \\ &= \left(\frac{b}{x}, -\frac{by}{x^2}\right) \end{aligned}$$

case 3 If $P_1 = P_2 = T$ then it is clear that

$$\phi(T+T) = \phi(T) + \phi(T)$$

Case 4 If $P_1, P_2 \notin \{\mathcal{O}, T\}$ and are distinct .
So in order to prove that ϕ is homomorphism it is now sufficient to show that if

$$P_1 + P_2 + P_3 = \mathcal{O}$$

then

$$\phi(P_1) + \phi(P_2)\phi(P_3) = \bar{\mathcal{O}}$$

because once we know this,then

$$\phi(P_1 + P_2) = \phi(-P_3) = -\phi(P_3) = \phi(P_1) + \phi(P_2)$$

since

$$\phi(-P) = \phi(x,-y) = \left(\Big(\frac{-y}{x}\Big)^2, \frac{-y(x^2-b)}{x^2}\right) = -\phi(x,y) = -\phi(P)$$

From the definition of the group law on a cubic curve, the condition $P_1 + P_2 + P_3 = \mathcal{O}$ is equivalent to the statement that P_1, P_2 and P_3 are co-linear, so let $= \lambda x + v$ be the line through them. We must show that $\phi(P_1), \phi(P_2)\text{and}\phi(P_3)$ are the intersection of some line with $\bar{E}$ The line intersecting $\bar{E}$ that we take is

$$y = \bar{\lambda}x + v \qquad \text{where} \qquad \text{and} \qquad \bar{v} = \frac{v^2 - av\lambda + b\lambda^2}{v}$$

To check, say, that $\phi(P_1) = \phi(x_1, y_1) = (\bar{x_1}, \bar{y_1})$ is on the line $y = \bar{\lambda}x + \bar{v}$, we just substitute and compute

$$\begin{aligned} \bar{\lambda}v_1 + \bar{v} &= \frac{v\lambda - b}{v}\Big(\frac{y_1}{x_1}\Big)^2 + \frac{v^2 - av\lambda + b\lambda^2}{v} \\ &= \frac{(v\lambda - b)y_1^2 + (v^2 - av\lambda + b\lambda^2)x_1^2}{vx_1^2} \\ &= \frac{(v\lambda(y_1^2 - ax_1^2) - b(y_1 - \lambda x_1)(y_1 - \lambda x_1) + vx_1^2}{vx_1^2} \end{aligned}$$

and now using $y_1^2 - ax_1^2 = x_1^3 + bx_1$ and $y_1 - \lambda x_1 = v$,we get

$$\begin{aligned}\bar{\lambda}v_1 + \bar{v} &= \frac{\lambda(x_1^3 + bx_1) - b(y_1 + \lambda x_1) + vx_1^2}{x_1^2} \\ &= \frac{x_1^2(\lambda x_1 + v) - by_1}{x_1^2} \\ &= \frac{(x_1^2 - b)y_1}{x_1^2} = \bar{y_1}\end{aligned}$$

Similarly we can compute for $\phi(P_2)$ and $\phi(P_3)$ Hence ϕ is homomorphism. □

Proof of (b). We noted above that the curve $\bar{\bar{E}}$ is given by the equation

$$\bar{\bar{E}} : y^2 = x^3 + 4ax^2 + 16bx$$

so it is clear that the map $(x, y) \longrightarrow (x/4, y/8)$ is an isomorphism from $\bar{\bar{E}}$ to E. From (a) there is a homomorphism $\bar{\phi} : \bar{E} \longrightarrow \bar{\bar{E}}$ defined by the same equations that define ϕ, but with $\bar{a}$ and $\bar{b}$ in place of a and b. Since the map $\psi : \bar{E} \longrightarrow E$ is the composition of $\bar{\phi} : \bar{E} \longrightarrow \bar{\bar{E}}$ with the isomorphism $\bar{\bar{E}} \longrightarrow E$, we get that $\bar{\psi}$ is a well-defined homomorphism from $\bar{E}$ to E. □

Proof of (c). Now we will prove that $\psi o \phi$ is multiplication by two.

$$2P = 2(x, y) = \left(\frac{(x^2 - b)^2}{4y^2}, \frac{(x^2 - b)(x^4 + 2ax^3 + 6bx^2 + 2abx + b^2)}{8y^3}\right)$$

and

$$\phi(x, y) = \left(\frac{y^2}{x^2}, \frac{y(x^2 - b)}{x^2}\right), \qquad \psi(\bar{x}, \bar{y}) = \left(\frac{\bar{y}^2}{4\bar{x}^2}, \frac{\bar{y}(\bar{x}^2 - b)}{8\bar{x}^2}\right)$$

So

$$\begin{aligned}\phi o\psi(x, y) &= \psi\left(\frac{y^2}{x^2}, \frac{y(x^2 - b)}{x^2}\right) \\ &= \left(\frac{\left(\frac{y(x^2-b)}{x^2}\right)^2}{4\left(\frac{y^2}{x^2}\right)^2}, \frac{\frac{y(x^2-b)}{x^2}\left(\left(\frac{y^2}{x^2}\right)^2 - (a^2 - 4b)\right)}{8\left(\frac{y^2}{x^2}\right)^2}\right) \\ &= \left(\frac{(x^2 - b)^2}{4y^2}, \frac{(x^2 - b)(y^4 - (a^2 - 4b)x^4)}{8y^3x^2}\right) \\ &= \left(\frac{(x^2 - b)^2}{4y^2}, \frac{(x^2 - b)(x^4 + 2ax^3 + 6bx^2 + 2abx + b^2)}{8y^3}\right) \\ \phi o\psi(x, y) &= 2(x, y) \\ &= 2P\end{aligned}$$

A similar computation gives $\phi o\psi(x, y) = 2(x, y)$. Since ϕ is a homomorphism, we know that

$$\phi(2P) = \phi(P + P) = \phi(P) + \phi(P) = 2\phi(P)$$

We just proved that $2P = \phi o\psi(P)$, so we get $\phi o\psi(\phi(P)) = 2(\phi(P))$. Now $\phi : E \longrightarrow \bar{E}$ is onto as a map of complex points, so for any $\bar{P} \in \bar{E}$ we can find $P \in E$ with $\phi(P) = \bar{P}$. Therefore $\phi o\psi(\bar{P}) = 2\bar{P}$. □

It is clear from the formulas that ϕ maps Γ into $\bar{\Gamma}$; but if you are given a rational point in $\bar{\Gamma}$, it is not at all clear if it comes from a rational point in Γ. If we apply the map ϕ to the rational points Γ, we get a

subgroup of the set of rational points Γ; we denote this subgroup by $\phi(\Gamma)$ and call it the image of Γ by ϕ. We make the following three claims, which taken together, provide a good description of the image.

Claim 3.3.9. **(i)** $\bar{\mathcal{O}} \in \phi(\Gamma)$.

(ii) $\bar{T} = (0,0) \in \phi(\Gamma)$ *iff* $\bar{b} = a^2 - 4b$ *is perfect square.*

(iii) *Let* $\bar{P} = (\bar{x}, \bar{y}) \in \bar{\Gamma}$ *with* $\bar{x} \neq 0$. *Then* $\bar{P} \in \phi(\Gamma)$ *iff* $\bar{x}$ *is the square of a rational number.*

Proof. **(i)** It is clear because $\bar{\mathcal{O}} = \phi(\mathcal{O})$

(ii) From the formula for ϕ we see that $\bar{T} \in \phi(\Gamma)$ if and only if there is a rational point $(x, y) \in \Gamma$ such that $y^2/x^2 = 0$. Note $x \neq 0$, because $x = 0$ means that $(x, y) = T$, and $\phi(T)$ is $\bar{\mathcal{O}}$, not $\bar{T}$. So$\bar{T} \in \phi(\Gamma)$ if and only if there is a rational point $(x, y) \in \Gamma$ with $x \neq 0$ and $y = 0$. Putting $y = 0$ in the equation for Γ gives

$$0 = x^3 + ax^2 + bx = x(x^2 + ax + b)$$

This equation has a non-zero rational root if and only if the quadratic equation $x^2 + ax + b$ has a rational root, which happens if and only if its discriminant $a^2 - 4b$ is a perfect square.

(iii) Let $\bar{P} \in \phi(\Gamma)$ is a point with $\bar{x} \neq 0$. From the definition of $\phi, \bar{x} = y^2/x^2$ is square of rational number conversely $\bar{x} = w^2$ for some rational number $w \in \mathbb{Q}$ we have to show that there exist a point $(x_1, y_1) \ni \phi(x_1, y_1) = (\bar{x}, \bar{y})$ We know that $\ker(\phi) = \{\mathcal{O}, T\}$.So there will be two points of Γ that map to it .Let

$$x_1 = \frac{1}{2}\Big(w^2 - a + \frac{\bar{y}}{w}\Big), \qquad y_1 = x_1 w$$

$$x_2 = \frac{1}{2}\Big(w^2 - a - \frac{\bar{y}}{w}\Big), \qquad y_2 = x_2 2w$$

Now we will claim that $P_i = (x_i, y_i) \in \Gamma$ and that $\phi(P_i) = (x_i, y_i)\ \forall\ i = 1, 2$.Now

$$\begin{aligned} x_1 x_2 &= \frac{1}{4}\Big((w^2 - a)^2 - \frac{\bar{y}^2}{w^2}\Big) \\ x_1 x_2 &= \frac{1}{4}\Big((\bar{x} - a)^2 - \frac{\bar{y}^2}{\bar{x}}\Big) \\ &= \frac{1}{4}\Big(\frac{\bar{x}^3 - 2a\bar{x}^2 + a^2\bar{x} - \bar{y}^2}{\bar{x}}\Big) \\ x_1 x_2 &= b \end{aligned}$$

Fr showing that $P_i = (x_i, y_i) \in \Gamma$ we have to show that

$$\frac{y_i^2}{x_i^2} = x_i + a + \frac{b}{x_i}$$

And also we have $\frac{y_i}{x_i} = \pm w$ and $x_1 x_2 = b$ So $w^2 = x_1 + a + x_2$ and from the definition of x_1 and x_2 we can find above expression .
It only remains to check that

$$\phi(P_i) = (x_i, y_i)$$

$$\frac{y_i^2}{x_i^2} = \bar{x} \qquad \text{and} \qquad \frac{y_i(x_i^2 - b)}{x_i^2} = \bar{y}$$

The expression follows from $\frac{y_i}{x_i} = \pm w$ and

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

$$\frac{y_2(x_2-b)}{x_2^2} = \frac{x_2 w(x_2^2 - x_1x_2)}{x_2^2} = w(x_1 - x_2)$$

and alsofrom the definition of x_1 and x_2

$$x_1 - x_2 = \frac{\bar{y}}{w} \Rightarrow w(x_1 - x_2) = \bar{y}$$

So $\frac{y_i(x_i^2-b)}{x_i^2} = \bar{y}$ Hence proved.

□

Lemma 3.3.10. **(a)** *The map* $\alpha : \Gamma \longrightarrow \mathbb{Q}^*/\mathbb{Q}^{*2}$ *defined by*

$$\alpha(\mathcal{O}) = 1 \mod Q^{*^2},$$

$$\alpha(T) = b \mod Q^{*^2},$$

$$\alpha(x, y) = x \mod Q^{*^2}$$

is a homomorphism if $x \neq 0$.

(b) *The kernel of* α *is the image* $\psi(\bar{\Gamma})$. *Hence* α *induces one-to-one homomorphism*

$$\frac{\Gamma}{\psi(\bar{\Gamma})} \hookrightarrow \frac{\mathbb{Q}^*}{\mathbb{Q}^{*2}}$$

(c) *Let* $p_1, p_2, \ldots, p_n$ *be the distinct primes dividing* b.*Then the image of* α *is contained in the subgroup of* $\frac{\mathbb{Q}^*}{\mathbb{Q}^{*2}}$ *consisting of the elements.*

$$\{\pm p_1^{\xi_1} p_2^{\xi_2} \ldots p_n^{\xi_n} : \text{ each } \xi \text{ equals } 0 \text{ or} 1\}$$

(d) *The* $[\Gamma : \phi(\bar{\Gamma})]$ *is at most* 2^{n+1}

Proof. **(a)**

$$\alpha(-P) = \alpha(x, -y) = x = \frac{1}{x} = \alpha(x, y)^{-1} = \alpha(P)^{-1} \mod Q^{*2}$$

For proving α is homomorphism it is enough to show that if $P_1+P_2+P_3 = \mathcal{O}$ then $\alpha(P_1).\alpha(P_2).\alpha(P_3) = 1 \mod Q^{*2}$

Suppose that $y = \lambda x + v$ is the line passing through P_1, P_2 and P_3 .If x_1, x_2 and x_3 are the x coordinate of the points P_1, P_2 and P_3 then from the derivation of duplication formula we know that

$$x_1.x_2.x_3 = v^2 + c$$

In our curve $c = 0$ so

$$x_1x_2x_3 = v^2 \in \mathbb{Q}^{*2}$$
$$x_1x_2x_3 = 1 \mod Q^{*2}$$
$$\alpha(P_1)\alpha(P_2)\alpha(P_3) = 1 \mod \mathbb{Q}^{*2}$$

(b) By the definition of $\alpha$with the description of $\psi(\bar{\Gamma})$ given in the claim 3.3.9 it is clear that kernel of α is precisely $\psi(\bar{\Gamma})$.

(c) We know that if $x = \frac{m}{e^2}$ and $y = \frac{n}{e^3}$ then

$$n^2 = m(m^2 + ame^2 + be^4)$$

Let

$$d = \gcd(m, m^2 + ame^2 + be^4)$$

So $d|b$ and $n^2 = m(m^2 + ame^2 + be^4)$

So we conclude that every prime dividing $m$appears to an even power except possibly for the primes dividing b therefore

$$m = \pm(\text{integer})^2 \prod_{i=1}^{n} P_i^{\xi_i}.$$

where $\xi \in \{0, 1\}$ and $P_i's$ are distinct

$$\alpha(P) = x \equiv \frac{m}{e^2} = \pm \prod_{i=1}^{n} P_i^{\xi_i} \mod \mathbb{Q}^{*2}.$$

Hence proved

(d) The subgroup deceived above has precisely 2^{n+1} elements and from (b) we have one-to-one homomorphism

$$\Gamma/\psi(\bar{\Gamma}) \to \mathbb{Q}^*/\mathbb{Q}^{*2}.$$

Hence the index of $\psi(\bar{\Gamma})$ in Γ is at most 2^{n+1} elements.

□

Lemma 3.3.11. *Let A and B be two Abelian groups,and consider two homomorphism $\phi(A) \longrightarrow B$ and $\psi : B \longrightarrow A$. Suppose that*

$$\psi o\phi(a) = 2a \qquad \forall\ a \in A \qquad\qquad \phi o\psi(b) = 2b \qquad \forall\ b \in B.$$

Suppose further that $\phi(A)$ has finite index in B ,and $\psi(B)$ has finite index in A. Then $2A$ has finite index in A. More precisely, the index satisfies

$$(A : 2A) \leq (A : \psi(B))(B : \phi(A)).$$

Proof. Since $\psi(B)$ has finite index in A, let $a_1, a_2, \ldots a_n$ representative for the cosets. Similarly, since $\phi(A)$ has finite index in B, let $b_1, b_2, \ldots, b_m$ representative for the cosets. We claim that the set

$$\{a_i + \psi(b_j) : 1 \leq i \leq n, 1 \leq j \leq m\}$$

includes a complete set of representatives for the cosets of $2A$ inside A. includes a complete set of representatives for the cosets of $2A$ inside A. To see this, let $a \in A$. We need to show that a can be written as the sum of an element of this set plus an element of $2A$. Since $a_1, a_2, \ldots, a_n$ are representatives for the cosets of $\psi(B)$ inside A, we can find some a_i so that $a - a_i \in' \psi(B)$, say $a - a_i = \psi(b)$. Next, since $b_1, b_2, \ldots, b_m$ are representatives for the cosets of $\psi(A)$ inside B, we can find some b_j so that $b - b_j \in \phi(A)$ say $b - b_j = \phi(a')$.Then

$$\begin{aligned} a &= a_i + \psi(b) = a_i + \psi(b_j + \phi(a')) \\ &= a_i + \psi(b_j) + \psi(\phi(a')) \\ &= a_i + \psi(b_j) + 2a' \end{aligned}$$

Hence the set

$$\{a_i + \psi(b_j) : 1 \leq i \leq n, 1 \leq j \leq m\}$$

is a complete set of representatives for the cosets of $2A$ inside A. □

Proof of proposition 3.3.7. By the lemmas 3.3.10, 3.3.11 we conclude that the index $[E(\mathbb{Q}) : 2E(\mathbb{Q})]$ is finte □

Theorem 3.3.12 (Mordell's theorem)**.** *Let E be an elliptic curve given by the equation*

$$E : y^2 = x^3 + ax^2 + bx + c,$$

where $a, b, c \in \mathbb{Q}$. Then the group $E(\mathbb{Q})$ is finitely generated abelian group.

Proof. By change of variable we can transform our elliptic curve $E : y^2 = x^3 + ax^2 + bx + c$, into $E' : y^2 = x^3 + ax^2 + bx$ over field $K(\neq 2)$. So E and E' are isomorphic so proving for E' is same as for E. From the lemma 3.3.1, 3.3.2, 3.3.5, 3.3.7 and descent theorem 3.3 we conclude that the group $E(\mathbb{Q})$ is finitely generated abelian group. □

3.4 Further developments

We have shown that the group Γ of rational points on the curve

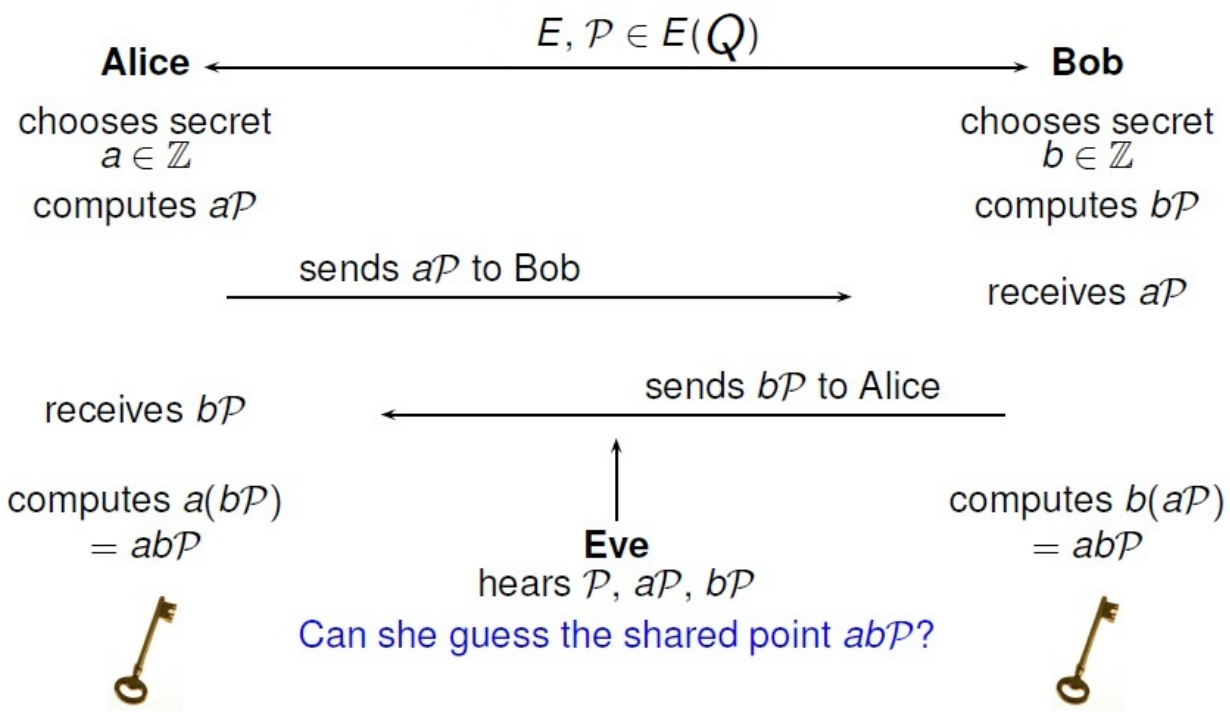
$$E : y^2 = x^3 + ax^2 + bx + c$$

is a finitely generated Abelian group. It follows from the fundamental theorem on Abelian groups that Γ is isomorphic, as an abstract group, to a direct sum of infinite cyclic groups and finite cyclic groups of prime power order. We will let $\mathbb{Z}$ denote the additive group of integers, and we will let $\mathbb{Z}/n\mathbb{Z}$ denote the cyclic group $\mathbb{Z}/m\mathbb{Z}$ of integers $\mod m$. Then the structure theorem tells us that Γ looks like

$$\Gamma \cong \mathbb{Z}^r \oplus \mathbb{Z}_{p_1^{v_1}} \oplus \mathbb{Z}_{p_2^{v_2}} \oplus \cdots \oplus \mathbb{Z}_{p_s^{v_s}}$$

where r is the **rank** of elliptic curve.

Motivation : Elliptic curve cryptography



Our security of elliptic curve cryptography depends on the question can she guess the shared point abP, where abP is addition of the point P ab times on elliptic curve.
If we take point P from an elliptic curve whose rank is 0 then this elliptic curve is useless for cryptography because of Mazur and Mordell's theorem.In this one she can guess the shared point abP very easily.
So if we take point P from an elliptic curve whose rank is at least 1. For guessing shared point abP is very very difficult if we take P very large number $\in \mathbb{Z}$ because point P has infinite order.

Chapter 4

Congruent Numbers

In this chapter we will discuss classical problem whether a natural number is congruent. We will see whether a natural number is congruent by the theory of elliptic curves.

4.1 Congruent number

Definition 4.1.1. *A natural number n is called* ***congruent number*** *if there exist a right angled triangle with all three sides rationals and with area n.*

Note 4.1.2. *Tunnel's theorem gives an almost complete answer to an ancient problem : find an simple test to determine whether or not a given natural number is the area of some right angled triangle all of whose sides are rational numbers.*

4.1.1 Method of generating Pythagorean triples

Their central discovery was that there is an easy way to generate all such triangles. Namely, take any two positive integers a and b with $a > b$, draw the line in the xy-plane through the point $(-1, 0)$ with slope b/a. Let (x, y) be the second point of intersection of this line with the unit circle.

$$y - 0 = \frac{y}{x}(x + 1) \Rightarrow y = \frac{y}{x}(x + 1)$$

and (x, y) lies on the circle so

$$u^2 + v^2 = 1 \qquad u^2 + \left(\frac{b}{a}\right)^2 (u + 1)^2 = 1$$
$$(a^2 + b^2)x^2 + 2b^2x + b^2 - a^2 = 0$$

so from the above equation we get

$$x = \frac{a^2 - b^2}{a^2 + b^2}$$
$$y = \frac{2ab}{a^2 + b^2}$$

then the integers $X = a^2 - b^2$, $Y = 2ab$ and $Z = a^2 + b^2$ are the sides of a right angular triangle follows from the equation of circle. So we can get all Pythagorean triples by taking all +ve integers a, b with $a > b$.**Conversely**, can be we find such two number with the help of given rational right angled triangle ?

Suppose we have rational right angled triangle with sides X,Y,Z.

$$X^2+Y^2=Z^2 \Rightarrow \left(\frac{X}{Z}\right)^2+\left(\frac{Y}{Z}\right)^2=1$$

Put $u=\frac{X}{Y}$ and $v=\frac{Y}{Z}$. (x,y) be any point on the circle(with center (0,0)and radius 1). Let $\frac{a}{b}$ be the slope of the line joining the points $(-1,0)$ and (u,v).
$\frac{Y}{Z}=\frac{b}{a}\left(\frac{X}{Z}+1\right)$ and $aY=b(X+Z)$ and $X^2+Y^2=Z^2$

4.1.2 Generalization of congruent number

If any natural number q is a congruent number, then s^2q is also a congruent number by multiplying the perpendicular legs each by s. Therefore we can observe that whether or not an number is a congruent number depends only on its residue class $\frac{\mathbb{Q}^+}{(\mathbb{Q}^+)^2}$ Every such residue class contains only one square-free number from which all other elements of that class can be derived, so it is a convention to only speak of square-free congruent numbers.

Problem 4.1.3. *Show that for $a,b\in\mathbb{Q}^+$, b is a congruent number if and only if a^2b is so.*

Proof. a is congruent number .
so by the congruent property there exist a right angular triangle with all rational sides X,Y,Z and with area a such that

$$X^2+Y^2=Z^2 \qquad \frac{1}{2}XY=b$$

Now scaling the sides of the triangle by $|a|$. let $X_1=aX$,$Y_1=aY$ and $Z_1=aZ$ then

$$X_1^2+Y_1^2=(aX)^2+(aY)^2=(aZ)^2=Z_1^2$$

and

$$\frac{1}{2}X_1Y_1=\frac{1}{2}(aX)(aY)=a^2\left(\frac{1}{2}XY\right)=a^2b$$
$$\Rightarrow \frac{1}{2}X_1Y_1=a^2b$$

so a^2b is a congruent number. Now suppose that a^2b is congruent number.then there exist a rational right triangle with sidesX_1,Y_1 and Z_1 such that

$$X_1^2+Y_1^2=Z_1^2$$
$$\frac{1}{2}X_1Y_1=a^2b$$

Claim 4.1.4. *b is congruent number.*

Proof.

$$\frac{1}{2}X_1Y_1=a^2b$$
$$\frac{1}{2}\frac{X_1}{a}\frac{Y_1}{a}=b$$

Let $X=\frac{X_1}{b}$, $Y=\frac{X_1}{b}Z=\frac{Z_1}{a}$ then

$$\frac{1}{2}XY=b$$

$$X_1^2+Y_1^2=Z_1^2 \Rightarrow (\frac{X_1}{a})^2+(\frac{Y_1}{a})^2=(\frac{Z_1}{a})^2 \Rightarrow X^2+Y^2=Z^2$$

hence b is congruent number. □

□

Theorem 4.1.5 (Tunnel's Theorem(1983)). *Let n be a square-free congruent number, i.e., n is the area of a right angled triangle. Define A_n, B_n, C_n, D_n as follows :*

(A) $A_n = \#\left\{(x,y,z) \in \mathbb{Z}^3 |\ 2x^2 + y^2 + 32z^2 = n\right\}$

(B) $B_n = \#\left\{(x,y,z) \in \mathbb{Z}^3 |\ 2x^2 + y^2 + 8z^2 = n\right\}$

(C) $C_n = \#\left\{(x,y,z) \in \mathbb{Z}^3 |\ 8x^2 + y^2 + 64z^2 = n\right\}$

(D) $D_n = \#\left\{(x,y,z) \in \mathbb{Z}^3 |\ 8x^2 + y^2 + 16z^2 = n\right\}$

Then

(i) $A_n = \frac{1}{2}B_n$ *if n is odd; and*

(ii) $C_n = \frac{1}{2}D_n$ *if n is even.*

If the Birch- Swinnerton - Dyer conjecture is true then these equalities imply that n is the congruent number and conversely.

Proposition 4.1.6. *By using the theorem above, let us show that the numbers $1, 2, 3$ and $4, 8$ are not congruent numbers but $5, 6$ and 7 are congruent numbers.*

Proof. For $n = 1, 3$, we see that $A_n = B_n = 1$. Hence, by Tunnell's Theorem above, the numbers $1, 3$ are not congruent. For $n = 2$ (resp., $n = 4$), we see that $C_n = D_n = 1$ (resp., $C_n = D_n = 2$). Again by the same theorem, the numbers $2, 4$ are also not congruent. Now we will show that $5, 6$ and 7 are congruent numbers.
The right angled triangle with sides $9, 40, 41$ and area $180 = 5.6^2$, so dividing the lengths by 6 produces the rational right angled triangle with sides $3/2, 20/3, 41/6$ and area 5. That is, 5 is a congruent number.The number $n = 6$ is a congruent number as one sees by considering the right angled triangle with sides $3, 4$ and 5. The right triangle with sides $175, 288, 337$ and area $25200 = 760^2$, so scaling by 60 produces the right angled triangle with sides $(35/12, 24/5, 337/60)$ with area 7. Thus 7 is a congruent number.From the previous result we know that a is congruent number if and only if ab^2 is congruent number. So 8 is not congruent number because $8 = 2.2^2$ □

Note 4.1.7. *The simplest rational right angled triangle with area 157 was computed by Don Zagier.*

Proposition 4.1.8. *Let n be a fixed square-free positive integer . Let X, Y, Z, x always denote rational number with $X < Y < Z$ .There is one-one correspondence between right angled triangle with legs X and Y and hypotenuse Z and area n ; and number x for which $x, x \pm n$ are each the square of a rational number . The correspondence is :*
$X, Y, Z \to x = (Z/2)^2$
$x \to X = \sqrt{x+n} - \sqrt{x-n}, Y = \sqrt{x+n} + \sqrt{x-n}, Z = 2\sqrt{x}.$
In particular , n is a congruent number if and only if there exist x such that x, $x + n$, $x - n$ re squares of rational numbers.

Proof. Let X,Y,Z is a triple of a right angled triangle and n is the area of this right angled triangle then we have

$$X^2 + Y^2 = Z^2$$
$$\frac{1}{2}XY = n$$

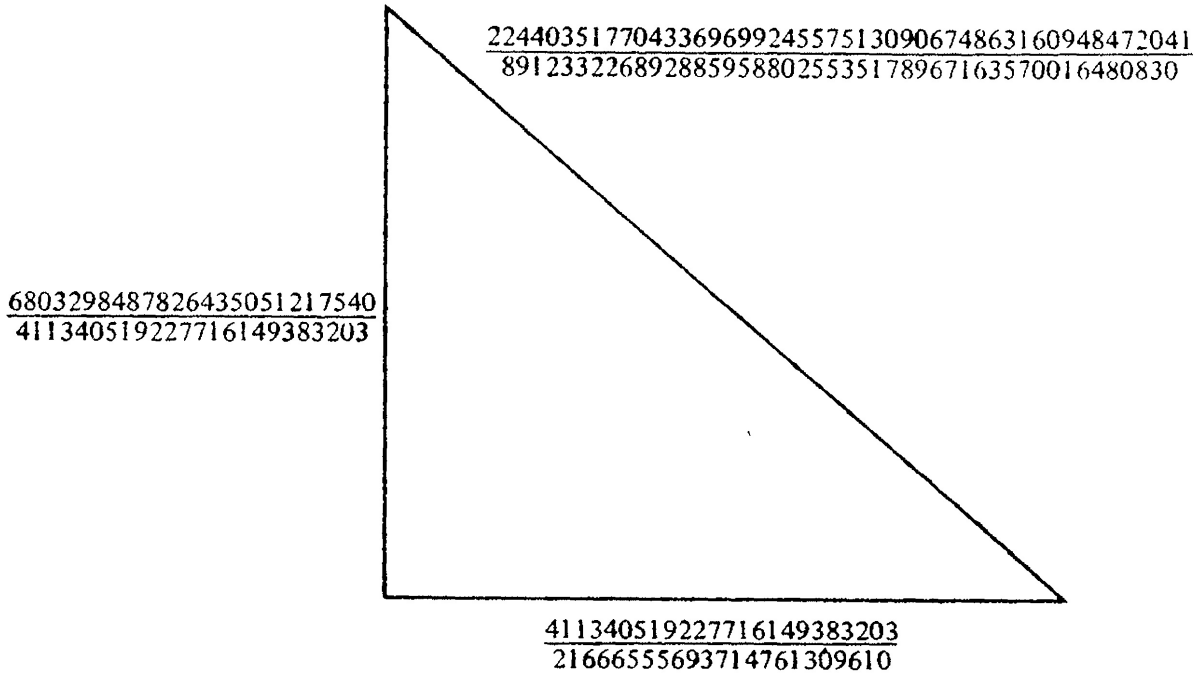


Figure I.3. The Simplest Rational Right Triangle with Area 157 (computed by D. Zagier).

If we add or subtract four times the second equation from the first, we obtain :

$$(X \pm Y)^2 = Z^2 \pm 4n$$

If then divide both sides by four, we see that $x = (Z/2)^2$ has the property that the numbers $x \pm n$ are the squares of $(X \pm Y)/2$. Conversely given x with given correspondence it is easy to check that the n is congruent number. Finally, to establish that the one-to-one correspondence , it only remains to verify that no two distinct triples X,Y,Z can lead to same x . For this, let two triples X,Y,Z and X_1,Y_1,Z_1 lead to same x .then

$$\begin{aligned} x &= (Z/2)^2 \\ x &= (Z_1/2)^2 \\ Z^2 &= Z_1^2 \\ \Rightarrow X^2 + Y^2 &= X_1^2 + Y_1^2 \end{aligned}$$

and

$$\frac{1}{2}XY = \frac{1}{2}X_1Y_1$$

then we find

$$\begin{aligned} (X \pm Y)^2 &= (X_1 \pm Y_1)^2 \\ X + Y &= X_1 + Y_1 \\ X - Y &= X_1 - Y_1 \end{aligned}$$

so we have

$$X = X_1, \qquad Y = Y_1 \qquad \text{and} \qquad Z = Z_1$$

□

4.2 A certain cubic equation

In the proof of proposition 1 we arrived at the equations

$$\left(\frac{X \pm Y}{2}\right)^2 = (Z/2)^2 \pm n$$

whenever X,Y,Z are the sides of right angled triangle with area n.So from these equations, we obtain

$$\big((X^2 - Y^2)/4\big)^2 = (Z/2)^4 - n^2$$

.this shows that the equation $u^4 - n^2 = v^2$ has a rational solution, namely, $u = Z/2$ and $v = (X^2 - Y^2)/4$.We next multiply by through u^2 to obtain $u^6 - n^2u^2 = (uv)^2$.If we set $x = u^2 = (Z/2)^2$ (this is the same x as in proposition 1) and further set $y = uv = (X^2 - Y^2)Z/8$, then we have a pair of rational numbers (x, y) satisfying the cubic equation : $y^2 = x^3 - n^2x$.
Thus, given a right angled triangle with rational sides X, Y, Z and area n, we obtain a point (x, y) in the xy -plane having rational coordinates and lying on the curve $y^2 = x^3 - n^2x$. Conversely, can we say that any point (x, y) with x,$y \in \mathbb{Q}$ which lies on the cubic curve must necessarily come from such a right triangle? Obviously not, because in the first place the x-coordinate $x = u^2 = (Z/2)^2$ must lie in $(\mathbb{Q}^+)^2$ if the point (x, y) can be obtained as in the last paragraph. To see this, notice that the right angled triangle having sides X, Y, Z can be obtained starting with a primitive Pythagorean triplet X_1, Y_1, Z_1 corresponding to a right angled triangle with integral sides X_1, Y_1, Z_1 and area s^2n, and then dividing the sides by s to get X, Y, Z. But in a primitive Pythagorean triple X and Y have different parity, and Z is odd. We conclude that $x = (Z/2)^2 = (Z_1/2s)^2$ has denominator divisible by 2 .
Finally a third condition is that the numerator of x have no common factor with n .To see this , suppose that $p > 2$ is a prime dividing both x and n. then p divides the numerator of

$$x \pm n = \left(\frac{X \pm Y}{2}\right)^2 \tag{4.1}$$

implies that

$$p|(X + Y)/2$$

and

$$\begin{aligned} p\,(X - Y)\,/2 \;&\Rightarrow\; p|X \;\&\; p|Y \\ &\Rightarrow p^2|XY \\ &\Rightarrow p^2|\frac{1}{2}XY = n \end{aligned}$$

but n was assumed as square-free integer. So we got contradiction. Hence, x is co-prime to n.

Note 4.2.1. *Now we will show that these three condition is not only necessary but also sufficient .*

Proposition 4.2.2. *Let (x,y) be a point with rational coordinates on the curve $y^2 = x^3 - n^2x$. Suppose that x satisfies the two conditions : (i) x is the square of a rational number, (ii)denominator of x is even and*

(iii)x is co-prime to n.Then there exists a right triangle with rational sides and area n which corresponds to x under the correspondence in Proposition 1

Proof. Let $u = \sqrt{x} \in \mathbb{Q}$. We work backwards through the sequence of steps at the beginning of this section. That is, set $v = y/u$, so that $v^2 = y^2/x = x^2 - n^2$,i.e.,$v^2 + n^2 = x^2$. Now let t be the denominator of u i.e., the smallest positive integer such that $tu \in \mathbb{Z}$. By assumption, t is even. Notice that the denominators of v^2 and x^2 are the same (because n is an integer and $v^2 + n^2 = x^2$), and this denominator is t^4. Thus, t^2v, t^2n, t^2x is a primitive Pythagorean triple, with t^2n even (primitivity follows from third condition). By Problem 1 of section 1, there exist integers a and b such that: $t^2n = 2ab$, $t^2v = a^2 - b^2, t^2 = a^2 + b^2$. Then the right triangle with sides $2/t$, $2/t$, 2 has area ab/t^2 , as desired. The image of this triangle $X = 2/t, Y = 2/t, Z = 2$ under the correspondence in Proposition 1 is $x = (Z/2)^2 = u^2$. This proves Proposition 2. □

Theorem 4.2.3. *The number $n \in \mathbb{N}$ is a congruent number if and only if the rank of the elliptic curve $y^2 = x^3 - n^2x$ is at least one.*

Proof. Let n be a congruent. We saw in Proposition 4.2.2 that n $x \in E(\mathbb{Q})$ so that $x(P) \in \mathbb{Q}^2$ .Since n is square-free, we have that$x(P) = 0, \pm n$. Thus, the point P cannot be in $E(\mathbb{Q})_{\text{tors}}$. This proves one direction of the theorem.
Suppose now that the rank of $E(\mathbb{Q})$ is at least one. This implies that there exists $P \in E(\mathbb{Q})$ with $y(P) \neq 0$. By the above proposition 4.1.8 corresponds to a triangle with area n. □

Chapter 5

Twists of elliptic curves of rank at least four

5.1 Introduction

In this chapter we give infinite families of elliptic curves over $\mathbb{Q}$ such that each curve has infinitely many non-isomorphic quadratic twists of rank at least 4. Assuming the Parity Conjecture, we also give elliptic curves over $\mathbb{Q}$ with infinitely many non-isomorphic quadratic twists of odd rank at least 5.

Mestre[Me92] showed that every elliptic curve over Q has infinitely many (non-isomorphic) quadratic twists of rank at least 2 over $\mathbb{Q}$ and he gave [Me98],[Me00] several infinite families of elliptic curves over $\mathbb{Q}$ with infinitely many (non-isomorphic) quadratic twists of rank at least 3. Further, he stated [Me98] that if E is an elliptic curve over $\mathbb{Q}$ with torsion subgroup isomorphic to $\mathbb{Z}/8\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, then there are infinitely many (non-isomorphic) quadratic twists of E with rank at least 4 over $\mathbb{Q}$.

Definition 5.1.1. *If $E : y^2 = f(x)$ is an elliptic curve , let E^d denote $dy^2 = f(x)$,the quadratic twist of E by d.*

Definition 5.1.2. *compositum or composite E_1E_2 of E_1 and E_2 is the intersection of all subfields of K containing both E_1 and E_2.*

Definition 5.1.3. *A field extension L/K is called algebraic if every element of L is algebraic over K, i.e. if every element of L is a root of some non-zero polynomial with coefficients in K.*

Definition 5.1.4. *A splitting field of a polynomial with coefficients in a field is a smallest field extension of that field over which the polynomial splits or decomposes into linear factors.*

Definition 5.1.5. *An algebraic field extension L/K is said to be normal if L is the splitting field of a family of polynomials in $K[X]$.*

Definition 5.1.6. *A Galois extension is an algebraic field extension E/F that is normal and separable; or equivalently, E/F is algebraic, and the field fixed by the automorphism group $Aut(E/F)$ is precisely the base field F. One says that such an extension is Galois.*

Definition 5.1.7. *A separable extension is an algebraic field extension $E \supset F$ such that for every $\alpha \in E$, the minimal polynomial of over F is a separable polynomial i.e., has distinct roots.*

Definition 5.1.8. *Galois group Suppose that E is an extension of the field F. An automorphism of E/F is defined to be an automorphism of E that fixes F pointwise. In other words, an automorphism of E/F is*

an isomorphism α from E to E such that $\alpha(x) = x$. for each x in F. The set of all automorphisms of E/F forms a group with the operation of function composition. This group is sometimes denoted by Aut(E/F). If E/F is a Galois extension, then Aut(E/F) is called the Galois group of (the extension) E over F, and is usually denoted by Gal(E/F).

Lemma 5.1.9. *Suppose that E is an elliptic curve over F , that $K_1, K_2, K_3, \ldots, K_n$ be the extension of F of degree at most 2 and that for $= 1, 2, 3, \ldots n$ there are points $P_i \in E(K_i)$ of infinite order. Suppose also that if $K_i \neq F$ then $\sigma(P_i) = -P_i$, where σ is the non trivial element of* Gal(K/F) *.Let K denote the compositum of $K_1, K_2, \ldots, K_n$. then $\{P_1, P_2, \ldots P_n\}$ is an independent set in $E(K)$.*

Proof. Let $G = \mathrm{Gal}(K/F)$ be a Galois group and define a map $\chi : \mathrm{Gal}(K_i/F) \to \{\pm 1\}$ denote the nontrivial character if $K_i \neq F$, and the trivial character if $K_i = F$ i.e., $\chi(f) = -1$ if $f \in F^c$ and $\chi(f) = 1$ if $f \in F$. Let $e_i = \sum_{\sigma \in G} \chi_i(\sigma)\sigma$. Then $\forall i$ and j,
Consider

$$e_i(P_j) = \sum_{\sigma \in G} \chi(\sigma)(\sigma(P_j))$$

$$= \sum_{\sigma \in G} \chi(\sigma)(\chi(\sigma)P_j) = \sum_{\sigma \in G} \chi(\sigma)\chi_j(\sigma)P_j = \begin{cases} 0, & \text{text}if \, i \neq j \\ |G|P_j, & \text{if} i = j \end{cases}$$

Suppose $\sum_j n_j P_j = O$. Then $O = e_i(\sum_j n_j P_j) = |G| n_i P_i \ \forall i$ Since P_i is of infinite order, $n_i = 0 \quad \forall i$
In the assumption we have assume that each P_i is of infinite order. So from above we conclude that $n_i = 0 \quad \forall \, i$. □

Definition 5.1.10. *If $k(t) \in \mathbb{Z}[t]$, we say that $k(t)$ is squarefree if $k(t)$ is not divisible by the square of any non constant polynomial in $\mathbb{Z}[t]$.*

Definition 5.1.11. *Suppose $g(t) \in \mathbb{Q}(t)$. A squarefree part of $g(t)$ is squarefree $k(t) \in \mathbb{Z}[t]$ such that $g(t) = k(t)j(t)^2$ for some $j(t) \in \mathbb{Q}(t)$.*

Proposition 5.1.12. *Suppose $f(x) \in \mathbb{Q}[x]$ is a separable cubic, and E is the elliptic curve $y^2 = f(x)$. Let $h_1(t) = t$, suppose we have non-constant $h_2(t) \ldots, h_r(t) \in \mathbb{Q}(t)$, let $k_i(t)$ be a squarefree part of $f(h_i(t))/f(t)$, and suppose that $k_1(t), \ldots, k_r(t)$ are distinct modulo $(\mathbb{Q}^*)^2$. Then*

1. *the rank of the rank of $E^{(f(t))}(\mathbb{Q}(t, \sqrt{k_2(t)}, \sqrt{k_2(t)}, \ldots, \sqrt{k_r(t)}))$ is at least r;*
2. *if C is the curve defined by the equations $s_i^2 = k_i(t)$ for $i = 1, \ldots, r$, then for all but at most finitely many rational points $(\tau, \sigma_1, \ldots, \sigma_r) \in C(\mathbb{Q})$, the rank of $E^{(f(t))}(\mathbb{Q})$ is at least r.*

Proof. Apply Lemma 2.1 to the elliptic curve $E^{(f(t))}$ over the field $F = \mathbb{Q}(t)$, with $K_i = F(\sqrt{k_i(t)})$ (so $K_1 = F$). Since the polynomials k_i are squarefree and distinct modulo $(\mathbb{Q}^*)^2$, the fields K_i are distinct. For $i = 1, \ldots, r$, let

$$P_i = (h_i(t), \sqrt{f(hi(t))/f(t)}) \in E^{(f(t))}(\mathbb{Q}(t, \sqrt{ki(t)})).$$

Note that P_i has infinite order, since its x-coordinate is not constant. Now (i) follows. □

5.2 Rank ≥ 4

From now on we consider elliptic curves of the form

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

where $\lambda \in \mathbb{Q} - \{0, 1\}$

Definition 5.2.1. *we fix a numbering of the linear fractional transformation $h_i(t) \in \mathbb{Q}(t)$ that permute the set $\{0, 1, \lambda\}$, along with corresponding squarefree parts $k_i(t)$:*

$$\begin{aligned} h_1(t) &= t & k_1(t) &= 1 \\ h_2(t) &= \tfrac{t-\lambda}{(2-\lambda)t-1}, & k_2(t) &= (1-\lambda)((\lambda-2)t-\lambda) \\ h_2(t) &= \tfrac{t-\lambda}{(2-\lambda)t-1}, & k_2(t) &= (1-\lambda)((\lambda-2)t-\lambda) \\ h_2(t) &= \tfrac{t-\lambda}{(2-\lambda)t-1}, & k_2(t) &= (1-\lambda)((\lambda-2)t-\lambda) \\ h_2(t) &= \tfrac{t-\lambda}{(2-\lambda)t-1}, & k_2(t) &= (1-\lambda)((\lambda-2)t-\lambda) \\ h_2(t) &= \tfrac{t-\lambda}{(2-\lambda)t-1}, & k_2(t) &= (1-\lambda)((\lambda-2)t-\lambda) \end{aligned}$$

Theorem 5.2.2. *Suppose $a \in \mathbb{Q} - \{1, -1, 0\}$and let $\eta = a^2$. Then*

$$f_\eta(x) = x(x-1)(x-\eta)$$

and let E_η be $y^2 = f(x)$. Let C_η be the curve
$v^2 = (\eta+1)^2u^4 + 4\eta(2\eta^2+3\eta+1)u^3 + 2(7\eta^4+7\eta^3+2\eta^2+\eta+1)u^2 + 4(2\eta^5+\eta^4-2\eta^2-\eta)u + (\eta^3-1)^2$
and let

$$t_\eta(u) = \frac{2(1-\eta)T_\eta(u)}{3((\eta+1)u^2+1-\eta^3)^2}$$

where
$T_\eta(u) = (\eta+1)^2u^4 + 2\eta(2\eta^2+3\eta+1)u^3 + 2(3\eta^4+3\eta^3+\eta^2+\eta+1)u^2 + 2\eta(\eta^3-1)(2\eta+1)u + \eta^6 - 2\eta^3 + 1$
Then:

1. *E_η and C_η are elliptic curves over $\mathbb{Q}$;*
2. *$\operatorname{rank}(C_\eta(\mathbb{Q})) \geq 1$;*
3. *for all but possibly finitely many $(u, v) \in C_\eta(\mathbb{Q})$, the quadratic twist of E_η by $f_\eta \circ t_\eta(u)$ has rank at least 4 over $\mathbb{Q}$;*
4. *there are infinitely many non-isomorphic quadratic twists of E_η of rank at least 4 over $\mathbb{Q}$.*

Proof. From the theorem 4.2(a) of [RS01] by noticing that when $\tau = \frac{2\lambda}{\lambda+1}$, then

$$\frac{k_3(\tau)}{k_2(\tau)} = \lambda^2 \text{and } k_2(\tau) = \frac{(\lambda-1)^2(2\lambda+1)}{\lambda+1}$$

We wanted $k_2(\tau)$ and $k_3(\tau)$ to be squares. Note that $\frac{-2\lambda+1}{\lambda+1} = a^2$ if and only if $\lambda = \frac{1-a^2}{2+a^2}$, and when these hold then $k_2(\frac{2\lambda}{\lambda+1})$ and $k_3(\frac{2\lambda}{\lambda+1})$ are both squares, and $(\frac{2\lambda}{\lambda+1}, (\lambda-1)a, \lambda(\lambda-1)a) \in C_{a^2} = C_\eta$. Further, we found that

$$\mathbb{Q}(t, \sqrt{k_2(t)}, \sqrt{k_3(t)}) = \mathbb{Q}(u)$$

with $t = t_\eta(u)$ as in the statement of this theorem. The curve C_η in the statement of this theorem is $v^2 = k_4(t_\eta(u))$. We observed that $(0, \eta^3 - 1) \in C_\eta(\mathbb{Q})$. We have

$$\mathbb{Q}(C_\eta) = \mathbb{Q}(u, \sqrt{k_4(t_\eta(u))} = \mathbb{Q}(t, \sqrt{k_2(t)}, \sqrt{k_3(t)}, \sqrt{k_4(t)})$$

By Proposition 5.1.12 (or Corollary 2.2 of [RS01] with $g_i(t) = k_i(t)f_\eta(t)$) the rank of $E_\eta^{f_\eta \circ t_\eta(u)}(\mathbb{Q}(C_\eta)$ is at least 4. By Proposition 5.1.12, the $E_\eta^{f_\eta \circ t_\eta(u))}(\mathbb{Q})$ is at least 4 for all but finitely many $(u, v) \in C_\eta(\mathbb{Q})$. More explicitly, for $i = 1, \ldots, 4$, write $f_\eta \circ h_i(t) = f_\eta(t)k_i(t)j_i(t)^2$ with $j_i(t) \in \mathbb{Q}(t)$. Then the points

$$(h_i \circ t_\eta(u), j_i \circ t_\eta(u)\sqrt{k_i \circ t_\eta(u)} \in E_\eta^{(f_\eta(t_\eta(u))}(\mathbb{Q}(u, v))$$

are

$$(t_\eta(u), 1)$$
$$\left(h_1 \circ t_\eta(u), \left(\frac{-(\eta+1)u^2+\eta^3-1}{a((\eta+1)u^2+2(\eta^2-1)u+\eta^3-1))}\right)^3\right)$$
$$\left(h_2 \circ t_\eta(u), \left(\frac{-(\eta+1)u^2+\eta^3-1}{a((\eta+1)u^2+2(\eta^2+\eta+1)u+\eta^3-1))}\right)^3\right)$$
$$\left(h_1 \circ t_\eta(u), \left(\frac{-(\eta+1)u^2+\eta^3-1}{v}\right)^3\right)$$

From the lemma 5.1.9 they give four independent points in $E_\eta^{(f_\eta \circ t_\eta(u))}(\mathbb{Q}(C_\eta))$. □

5.3 Root number

Definition 5.3.1. *If E is an elliptic curve over $\mathbb{Q}$, let N_E denote the conductor of E, let w_E denote the global root number, i.e., the sign in the functional equation for $L(E,s)$, and let $w_{E,p}$ denote the local root number at a prime $p \leq \infty$. Write $w_E(d)$ for $w_{E^{(d)}}$ and write $w_{E,p}(d)$ for $w_{E^{(d)},p}$.*

Definition 5.3.2. *If $\alpha \in \mathbb{Q}\times$ and $n \in \mathbb{Z}^+$, then:*

1. *$\alpha \equiv 1 \bmod^\times n$ means that $\alpha - 1 \in n\mathbb{Z}$ for all primes $l|n$;*

2. *$\alpha \equiv 1 \bmod^\times n\infty$ means that $\alpha \equiv 1 \bmod^\times n$ and $\alpha > 0$.*

Lemma 5.3.3. *Suppose E is an elliptic curve over $\mathbb{Q}, d, d' \in \mathbb{Q}^*$, and there exists $\beta \in \mathbb{Q}^*$ such that $\beta^2 d/d' \equiv 1 \bmod^\times 8N_{E\infty}$. Then $w_E(d) = w_E(d')$.*

Proof. Taking the squarefree parts of d and d , we can reduce to the case where d and d are squarefree integers. If $p < \infty$ and $p \nmid dN_E$, then $E^{(d)}$ has good reduction over $\mathbb{Q}_p$, so $w_{E,p}(d) = 1$ (see Proposition 2(iv) of [R93]). Similarly for d' . Thus,

$$w_E(d) = \prod_{p \leq \infty} w_{E,p}(d) = \prod_{p|dN_{E\infty}} w_{E,p}(d)$$

If d/d' is a square in $\mathbb{Q}_p^*$, then $E^{(d)}$ and $E^{(d')}$ are isomorphic over $\mathbb{Q}_p$, so $w_E, p(d) = w_{E,p}(d)$ for all $p \geq \infty$. In particular, since $d/d' > 0$, it follows that $w_{E,\infty}(d) = w_{E,\infty}(d)$. If $p|2N_E$, then d/d' is a square in $\mathbb{Q}^*p$ (since $\beta^2 d/d' \equiv 1 \bmod^\times 8N_E$), so $w_{E,p}(d) = w_{E,p}(d)$. If $p|2N_E$, then p divides d if and only if p divides d (since $2\mathrm{ord}_p(\beta) + \mathrm{ord}_p(d) = \mathrm{ord}_p(d)$, and d and d are squarefree). Thus,

$$\frac{\prod_{p|dN_{E\infty}} w_{E,p}(d)}{\prod_{p|dN_{E\infty}} w_{E,p}(d')} = \frac{\prod_{p|d,p|2N_E} w_{E,p}(d)}{\prod_{p|d,p|2N_E} w_{E,p}(d)}$$

Suppose $p \nmid N_E$, so E has good reduction at p. Since E and $E(d)$ has good reduction at p. If E and $E(d)$ are isomorphic over $\mathbb{Q}_p(d), E^{(d)}$ has good reduction over $\mathbb{Q}_p(d)$. If $p|d$, then $\mathbb{Q}_p(\sqrt{d})$ is the smallest extension of $\mathbb{Q}_p$ over which $E^{(d)}$ has good reduction (and similarly for d). By (iii) and (v) of Proposition 2 of [R93] with $e = 2$, we have

$$w_E, p(d) = \frac{-1}{p}$$

if $p|d$ and $p \nmid 2N_E$, where $\frac{-1}{m}$is the Jacobi symbol. So from above we have

$$\frac{w_E(d)}{w_E(d')} = \frac{\prod_{p|d,p|2N_E} \frac{-1}{p}}{\prod_{p|d,p|2N_E} \frac{-1}{p}}$$

where $f = d/\gcd(d, 2N_E)$ and $f = d'/\gcd(d', 2N_E)$. Note that $f/f' = d/d'$. Then $\beta^2 f/f' \equiv 1 \mathrm{mod}^{\times} 4$, so $f \equiv f'(\mathrm{mod} 4)$, so $\frac{1}{f} = \frac{1}{f'}$ □

Lemma 5.3.4. *Suppose E and B are elliptic curves over $\mathbb{Q}, B(\mathbb{Q})$ has infinite order,$P \in B(\mathbb{Q}), r$ is a rational function in $\mathbb{Q}(B)$, and P is not a zero or pole of r. Then there exist a $Q \in B(\mathbb{Q})$ of infinite order and an open neighborhood U of O in $B(\mathbb{R})$ such that if $k \in \mathbb{Z}$ and $kQ \in U$ then $w_E(r(P+kQ)) = w_E(r(P))$.*

Lemma 5.3.5. *Suppose B is an elliptic curve over $\mathbb{Q}, Q \in B(\mathbb{Q})$ is a point of infinite order, and U is an open subset of the identity component $B(\mathbb{R})^0$ of $B(\mathbb{R})$. Then $\{k \in \mathbb{Z} : kQ \in U\}$ is infinite.*

Proof. Replacing Q by $2Q$, we may assume that $Q \in B(\mathbb{R})^0$. Note that $B(\mathbb{R})^0$ is isomorphic to the unit circle in $\mathbb{C}^*$, so every infinite subgroup is dense. Thus $\{kQ : k \in \mathbb{Z}\}$ is dense in $B(\mathbb{R})^0$, and the lemma follows. □

5.4 Rank ≥ 5

Theorem 5.4.1. *Suppose $a \in \mathbb{Q} - \{0, 1, 1\}$ and $\eta = a^2$. Suppose E_η, f_η , and t_η are as in Theorem 5.2.2. If $w_{E_\eta}(f_\eta.t_\eta(u_1)) = -1$ for some $(u_1, v_1) \in B_\eta(\mathbb{Q})$, and the Parity Conjecture holds for all quadratic twists of E_η , then E_η has infinitely many non-isomorphic quadratic twists of odd rank ≥ 5 over $\mathbb{Q}$.*

Proof. Let $P = (u_1, v_1)$, and let $r(z) = f_\eta \circ t_\eta \circ x(z) \in \mathbb{Q}(B_\eta)$, where the function x gives the x-coordinate of a point. By Lemmas 5.3.4 and 5.3.5 with $E = E_\eta$ and $B = B_\eta$, there are $Q \in B_\eta(\mathbb{Q})$ and infinitely many $k \in \mathbb{Z}$ such that

$$w_{E_\eta}(r(P + kQ)) = w_{E_\eta}(r(P)) = -1,$$

so by the Parity Conjecture, $E_\eta^{r(P+kQ)}(\mathbb{Q})$ has odd rank.
By Theorem 5.2.2, for all but finitely many $k \in \mathbb{Z}$, the rank of $E_\eta^{(r(P+kQ))}(\mathbb{Q})$ is at least 4. Thus for infinitely many k, the rank of $E_\eta^{(r(P+kQ))}(\mathbb{Q})$ is at least 5. As argued in the proof of Theorem 5.2.2, for each squarefree $d \in \mathbb{Q}^*$, the set of $u \in \mathbb{Q}$ such that $f_\eta \circ t_\eta(u)$ and d differ by a rational square is finite, since the hyperelliptic curve $f_\eta \circ t_\eta(u) = dz^2$ has only finitely many rational solutions (u, z). Thus there are infinitely many non-isomorphic quadratic twists of E_η of odd rank at least 5 over $\mathbb{Q}$. □

Chapter 6

The Selmer group, the Shafarevitch-Tate group

6.1 Group cohomology

Firstlly we will define some basic definition which we will use in this chapter.

Definition 6.1.1 (Topological group)**.** *A topological group G is a group that is also a topological space such that the product map:*

$$p : G \times G \longrightarrow G$$

$$(g, g') \longmapsto gg'$$

and the inverse map

$$i : G \longrightarrow G$$

$$g \longmapsto g^{-1}$$

are continuous functions (with respect to the topology).

Definition 6.1.2 (Profinite group)**.** *A Profinite group is a compact, Hausdorff and totally disconnected topological group.*

Definition 6.1.3 (Group cohomology H^0)**.** *Let G be a profinite group. Let A be a (discrete, left) G-module and that the map $G \times A \longrightarrow A$ is continuous when A is given the discrete topology. Define A^G and $\mathrm{H}^0(G, A)$ by*

$$A^G = \mathrm{H}^0(G, A) := \{a \in A : ga = a \ \ \forall\ g \in G\}$$

. The subgroup A^G is known as the subgroup of G-invariants of A.‘

Definition 6.1.4. *Let A be a G module. The group of i-cochains(from G to M) is defined by*

$$C^1(G, M) = \{\text{maps } f : G \to M\}$$

The group of i-cocycles (from G to M) is given by

$$Z^1(G, M) = \{f \in C^1(G, M) : \ \ f(gh) = hf(g) + f(h) \ \forall\ f, g \in G\}$$

The group of i-coboundaries (from G to M) is defined by

$$B^1(G,M) = \{f \in C^1(G,M) : \text{there exist an } m \in M \text{ such that } f(g) = gm - m \ \forall g \in G\}$$

It is clear that $B^1(G,M) \subseteq Z^1(G,M)$.

6.2 Cohomology group ($\mathrm{H}^i : i > 0$)

The i-th cohomology group of the G-module M is the quotient group

$$\frac{Z^1(G,M)}{B^1(G,M)}$$

Remark 6.2.1. *Notice that if the action of G on M is trivial, then*

$$\mathrm{H}^0(G,M) = M \qquad\qquad \mathrm{H}^1(G,M) = \mathrm{Hom}(G,M).$$

Definition 6.2.2. *In the context of group theory, a sequence*

$$G_0 \to G_1 \to G_2 \cdots \to G_n$$

of groups and group homomorphisms is called exact if the image of each homomorphism is equal to the kernel of the next. Note that the sequence of groups and homomorphisms may be either finite or infinite.

Remark 6.2.3.

1. *The sequence $0 \to A \to B$ is exact at A if and only if the map from A to B has kernel 0, i.e. if and only if that map is a monomorphism (one-to-one).*

2. *the sequence $B \to C \to 0$ is exact at C if and only if the image of the map from B to C is all of C, i.e. if and only if that map is an epimorphism (onto).*

3. *A consequence of these last two facts is that the sequence $0 \to X \to Y \to 0$ is exact if and only if the map from X to Y is an isomorphism.*

Remark 6.2.4. *Suppose that*

$$0 \to A \to B \to C \to 0$$

is an exact sequence of G-modules. This means that the morphisms respect the G-actions, and that it is exact as a sequence of abelian groups. Then there is an exact sequence

$$0 \to A^G \to B^G \to C^G \tag{1}$$

but one cannot always append $\to 0$ to the right end. In other words, the functor $A \to A^G$ is only left exact.

Theorem 6.2.5. *There exists a collection of functors $\mathrm{H}^i(G,-)$ for $i \geq 0$ such that for every exact sequence*

$$0 \to B \to C \to 0$$

where A, B and C are of G module, the sequence 1 extends to a long exact sequence

$$0 \to \mathrm{H}^0(G,A) \to \mathrm{H}^0(G,B) \to \mathrm{H}^0(G,C) \to$$
$$\mathrm{H}^1(G,A) \to \mathrm{H}^1(G,B) \to \mathrm{H}^1(G,C) \to$$
$$\mathrm{H}^2(G,A) \to \dots,$$

functorially with respect to the exact sequence. Functorially means that given a morphism of exact sequences, that is, a commutative diagram such as

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A & \longrightarrow & B & \longrightarrow & C & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & A' & \longrightarrow & B' & \longrightarrow & C' & \longrightarrow & 0, \end{array}$$

there is a morphism of the associated long exact sequences; that is, the diagram

$$\begin{array}{ccccccccccc} 0 & \longrightarrow & \mathrm{H}^0(G,A) & \longrightarrow & \mathrm{H}^0(G,B) & \longrightarrow & \mathrm{H}^0(G,C) & \longrightarrow & \mathrm{H}^1(G,A) & \longrightarrow & \dots \\ & & \downarrow & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & \mathrm{H}^0(G,A') & \longrightarrow & \mathrm{H}^0(G,B') & \longrightarrow & \mathrm{H}^0(G,C') & \longrightarrow & \mathrm{H}^1(G,A') & \longrightarrow & \dots, \end{array}$$

commutes.

Remark 6.2.6. *Let m is an integer not divisible by the characterstic of k and μ_m denotes the group of m-th root of unity then by using Hilbert 90 theorem we can see that*

$$\mathrm{H}^1(G_k, \mu_m) \simeq k^*/(k^*)^m$$

Definition 6.2.7. *A valuation on a field K is a function $\phi : K \to \mathbb{R} \geq 0$ satisfying:*

1. $\phi(x) = 0$ iff $x = 0$;
2. $\phi(xy) = \phi(x)\phi(y)\ \forall\ x, y \in K$;
3. *there exists $C \in \mathbb{R} > 0$ suc that*
   $\phi(x+y) \leq C\max\{\phi(x), \phi(y)\}\ \forall\ x, y \in K$.

The smallest constant C that can be taken in (iii) is the norm of the valuation ϕ. It obviously can not be smaller than 1. Note that if ϕ is a valuation on K of the norm C then $x \longmapsto \phi(x)^r$ defines a valuation of norm C^r on K for each $r \in \mathbb{R} > 0$.

6.3 Restriction

If $H \subseteq G$ is a closed subgroup, and A is a G-module, then A can also be considered as an H-module, and there exist restriction homomorphisms

$$\mathrm{H}^i(G,A) \xrightarrow{\mathrm{Res}} \mathrm{H}^i(\mathrm{H},A)$$

for each $i \geq 0$. On H^0, Res is simply the inclusion $A^G \hookrightarrow A^{\mathrm{H}}$. On H^1 , Res maps the class of the 1-cocycle $\xi : G \to A$ to the class of $\xi|_{\mathrm{H}} : \mathrm{H} \to A$. For us, the following special case will be important. Let k be a

number field. Let k_v denote the completion of k at a place v. If we identify $\bar{k}$ with the algebraic closure of k inside k_v , then we have an injection

$$G_v := \mathrm{Gal}(\bar{k_v}/k_v) \hookrightarrow G_k := \mathrm{Gal}(\bar{k}/k)$$

$$\sigma \to \sigma|_k$$

whose image is a decomposition group at v. Let A be an abelian variety over k. The composition

$$\mathrm{H}^1(k, A) := \mathrm{H}^1(G_k, A(\bar{k})) \xrightarrow{\mathrm{Res}} \mathrm{H}^1(G_v, A(\bar{k})) \to \mathrm{H}^1(G_v, A(\bar{k_v})) =: \mathrm{H}^1(k_v, A)$$

is denoted Res_v

Definition 6.3.1 (Perfect field)**.** *a field K is said to be perfect if every irreducible polynomial over K has distinct roots or every irreducible polynomial over K is separable.*

6.4 Twists (also known as k-forms)

Let k be a perfect field. Let V be an object over k, for example a variety equipped with some extra structure defined over k. We assume that the objects form a category, and that there is a notion of base extension: that is, given an object V over k and a field extension L of k, there should be an associated object V_L over L. A twist or k-form of V is an object W over k such that there exists a (structure-preserving) isomorphism $W_{\bar{k}} \simeq V_{\bar{k}}$ of objects over k. Then there is an injection

$$\{\text{twists of } V\} \hookrightarrow \mathrm{H}^1(G_k, \mathrm{Aut}(V_{\bar{k}}))$$

that in many situations is a bijection. Where we write "twists of V" we identify two twists if they are isomorphic over k.

6.5 The Shafarevich-Tate group

From now on, we assume that k is a number field, and that A is an abelian variety over k. Recall that there is a restriction map Res $v : \mathrm{H}^1(k, A) \to \mathrm{H}^1(k_v, A)$ for each place v of k (finite or infinite). If we identify elements of H^1 with torsors, then Res_v takes a k-torsor X under A to the base extension $X \times_k k_v$. Define the Shafarevich-Tate group $X(k, A)$ of$A$ over k as

$$\ker\Big[\mathrm{H}^1(k, A) \xrightarrow{Res} \prod_{\text{place } v \text{ of } k} \mathrm{H}^1(k_v, A)\Big]$$

where $\mathrm{Res} = \prod_v \mathrm{Res}_v$. Call a k-torsor X under A locally trivial if it is in the kernel of every map Res_v , or equivalently if $X(k_v)$ is nonempty for every v. Then one can describe $X(k, A)$ geometrically as the set of isomorphism classes of locally trivial k-torsors X under A.
Conjecture For every number field k and every abelian variety A over k, the group $Ш(k, A)$ is finite.

6.6 The Selmer Group

Fix an integer $m \geq 2$. For any abelian group B, let B_m denote the kernel of the multiplication-by-m map $B \to B$. Suppose that A is an abelian variety over a perfect field k. Then the m-torsion subgroup of

A is the G_k-module $A_m := A(\bar{k})m$. The long exact sequence associated to

$$0 \to A_m \to A(\bar{k}) \xrightarrow{m} A(\bar{k}) \to 0$$

from which we extract the top row of

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \frac{A(k)}{m} & \longrightarrow & \mathrm{H}^1(k, A_m) & \xrightarrow{\rho} & \mathrm{H}^1(k, A)_m & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow{\scriptstyle \mathrm{Res}} & \searrow^{\bar{\rho}} & \downarrow{\scriptstyle \mathrm{Res}} & & \\
0 & \longrightarrow & \prod_v \frac{A(k_v)}{m} & \longrightarrow & \prod_v \mathrm{H}^1(k_v, A_m) & \longrightarrow & \prod_v \mathrm{H}^1(k_v, A)_m & \longrightarrow & 0,
\end{array}$$

The bottom row is the product of the analogous sequences over each completion k_v. The first vertical map is induced by the inclusions $A(k) \hookrightarrow A(k_v)$ for each v, and the other vertical maps are restriction maps. The diagonal dotted map $\bar{\rho}$ is the composition in either direction. The diagram commutes. If we could prove that $\mathrm{H}^1(k, A_m)$ were finite, then (2) would show that $A(k)/m$ is finite too, and we would have proved the Weak Mordell-Weil Theorem. But unfortunately, it turns

out that $\mathrm{H}^1(k, A_m)$ is infinite whenever A is nonzero. Therefore we must bound the image of$A(k)/m$ in $\mathrm{H}^1(k, A_m)$ by using (2) to see that this image equals $\ker(\rho)$. Unfortunately, it is not known how to decide, given an element of $\mathrm{H}^1(k, A_m)$, whether its image in $\mathrm{H}^1(k, A)_m$ is zero or not, just as it is not known how to decide whether a general element of $\mathrm{H}^1(k, A)$ is zero or not. Therefore we instead bound $\ker(\rho)$ by the larger group $\ker(\bar{\rho})$: this helps, since given $\xi \in \mathrm{H}^1(k, A_m)$, we can decide whether $\xi \in ker(\bar{\rho})$ as follows: compute a torsor X representing its image in $\mathrm{H}^1(k, A)$, and use the method discussed in the previous section to test whether X is locally trivial. The m-Selmer group $\mathrm{Sel}^m(A/k)$ is defined as $\ker(\bar{\rho}\,)$, or equivalently as the set of $\xi \in \mathrm{H}^1(k, A_m)$ whose restriction $\mathrm{Res}_v \in \mathrm{H}^1(k_v, A_m)$ is in the image of $\frac{A(k_v)}{m} \to \mathrm{H}^1(k_v, A_m)$ for every v. If we apply the Snake Lemma to

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \frac{A(k)}{m} & \longrightarrow & \mathrm{H}^1(k, A_m) & \longrightarrow & \mathrm{H}^1(k, A)_m & \longrightarrow & 0 \\
 & & \downarrow & & \vdots{\scriptstyle \bar{\rho}} & & \downarrow{\scriptstyle \mathrm{Res}} & & \\
0 & \longrightarrow & 0 & \longrightarrow & \prod_v \mathrm{H}^1(k_v, A_m) & = & \prod_v \mathrm{H}^1(k_v, A)_m & \longrightarrow & 0,
\end{array}$$

the first half of the snake (i.e., the sequence of kernels of the vertical maps) is the fundamental exact sequence

$$0 \to \frac{A(k)}{m} \to \mathrm{Sel}^m(A/k) \to Ш_m \to 0,$$

where $Ш := Ш(k, A)$. In particular, the image of $A(k)/m$ in $\mathrm{H}^1(k, A_m)$ is contained in $\mathrm{Sel}^m(A/k)$.

6.7 Computing the Selmer group

Theorem 6.7.1. *The group* $\mathrm{Sel}^m(A/k)$ *is finite and computable (in theory)*

Corollary 6.7.2. *The groups* $A(k)/m$ *and* $Ш_m$ *are finite (but not necessarily computable).*

6.8 2-descent on an elliptic curve with rational 2-torsion

In this section we show how to compute $\mathrm{Sel}^2(A/k)$ in the case where $A = E$ is an elliptic curve over $\mathbb{Q}$ with $E_2 \subseteq E(\mathbb{Q})$. Then E has an equation

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

where $e_1, e_2, e_3 \in \mathbb{Z}$ are distinct. Let $P_i = (e_i, 0) \in E(\mathbb{Q})$ and let O denote the identity of E (the point at infinity). Then

$$E_2 = \{O, P_1, P_2, P_3\} = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} = \mu_2 \times \mu_2$$

as G_Q -modules, with $P_1 \leftrightarrow (1, -1)$ and $P_2 \leftrightarrow (-1, 1)$.So from Hilbert 90 theorem, $\mathrm{H}^1(\mathbb{Q}, \mu_2) \simeq \mathbb{Q}^*/\mathbb{Q}^{*2}$, so $\mathrm{H}^1(\mathbb{Q}, E_2) \simeq (\mathbb{Q}^*/\mathbb{Q}^{*2})^{\oplus 2}$. If p is a prime such that e_1, e_2, e_3 are distinct modulo p, then E has good reduction at p. Hence we may take as the set S of bad places in the previous section, the set consisting of the archimedean place ∞ and the primes dividing $2(e_1 - e_2)(e_2 - e_3)(e_3 - e_1)$. We then have the following facts:

1. If $\xi \in \mathrm{H}^1(\mathbb{Q}, E_2)$ corresponds to the image of $(a, b) \in (\mathbb{Q}/\mathbb{Q}^{*2})^{\oplus 2}$ (where $a, b \in \mathbb{Q}^{*2}$), then ξ is unamified at a prime p if nd only if p is unramified in the quadratic extension $\mathbb{Q}(\sqrt{a})$ and $\mathbb{Q}(\sqrt{b})$ of $\mathbb{Q}$.

2. The composition

$$E(\mathbb{Q}) \to E(\mathbb{Q})/2 \hookrightarrow \mathrm{H}^1(\mathbb{Q}, E_2) \simeq (\mathbb{Q}^*/\mathbb{Q}^{*2})^{\oplus 2}$$

maps a point (x, y) in $E(\mathbb{Q})$ other than O, P_1, P_2 to $(x - e_1, x - e_2) \in (\mathbb{Q}^*/\mathbb{Q}^{*2})^{\oplus 2}$.

It follows from (1) that $\xi \in \mathrm{H}^1(\mathbb{Q}, E_2)$ is unramified outside S if and only if ξ is represented by some pair (a, b) of elements in the subgroup $\langle -1, S\rangle$ of $\mathbb{Q}^*/\mathbb{Q}^{*2}$ generated by -1 and the finite primes of S. Thus

$$\mathrm{Sel}^2(E/\mathbb{Q}) \subseteq \mathrm{H}^1(\mathbb{Q}, E_2; S) \simeq \langle -1, S\rangle^{\oplus 2} \subset (\mathbb{Q}^*/\mathbb{Q}^{*2})^{\oplus 2}$$

To decide which $(a, b) \in \langle -1, S\rangle^{\oplus 2}$ actually belong to $\mathrm{Sel}^2(E/\mathbb{Q})$, check whether $X_{a,b}$ has points over R and over $\mathbb{Q}_p$ for all finite primes $p \in S$

Example 6.8.1. *Let E be the elliptic curve $y^2 = x^3 - x$ over $\mathbb{Q}$. Let r be the rank of $E(\mathbb{Q})$. We will compute $r, \mathrm{Sel}^2(E/Q)$, and $Ш(\mathbb{Q}, E)_2$. Take $e_1 = -1, e_2 = 0, e_3 = 1$. Then we may take $S = \{\infty, 2\}$. The homomorphism*

$$E(\mathbb{Q})/2 \to \mathrm{Sel}^2(E/\mathbb{Q}) \subseteq \mathrm{H}^1(\mathbb{Q}, E_2; S) \simeq \langle -1, 2\rangle^{\oplus 2} \subset (\mathbb{Q}^*/\mathbb{Q}^{*2})^{\oplus 2}$$

maps

$$O \to (1, 1)$$
$$P_1 = (-1, 0) \to (2, -1)$$
$$P_2 = (0, 0) \to (1, -1)$$
$$P_3 = (1, 0) \to (2, 1)$$

so at least these images are contained in $\mathrm{Sel}^2(E/\mathbb{Q})$. Now, for the other $(a, b) \in \langle -1, 2\rangle^{\oplus 2}$ we must check whether $X_{a,b}$ has points over $\mathbb{R}$ and $\mathbb{Q}_2$. An affine piece of $X_{a,b}$ is given by the equations

$$x + 1 = az_1^2,\ x = bz_2^2,\ x - 1 = abz_3^2,$$

and it will suffice to check this piece for points over $\mathbb{R}$ and $\mathbb{Q}_2$, because when a smooth curve over a local field has a point, the implicit function theorem implies that the curve has an analytic neighborhood of such points. If $a < 0$ and $X_{a,b}$ has a real point, the first equation shows that it satisfies $x \leq 1$, the second equation shows that $b < 0$, and the third equation yields a sign contradiction. Thus

$$\{(1, 1), (2, 1), (1, 1), (2, 1)\} \subseteq \mathrm{Sel}^2(E/\mathbb{Q}) \subseteq \langle 2\rangle \times \langle -1, 2\rangle.$$

But $\mathrm{Sel}^2(E/\mathbb{Q})$ is a group, so it equals either the group of order 4 on the left, or the group of order 8 on the right. A calculation shows that $X_{1,2}(\mathbb{Q}_2)$ is empty, so $\mathrm{Sel}^2(E/\mathbb{Q}) = \{(1, 1), (2, -1), (1, -1), (2, 1)\}$. Since $E(\mathbb{Q})/2 \to \mathrm{Sel}^2(E/\mathbb{Q})$ is surjective, $Ш(\mathbb{Q}, E)_2 = 0$. Finally, since $E_2 \subseteq E(\mathbb{Q}), \#(E(\mathbb{Q})/2) = 2^{2+r}$. On the other hand, $\#(E(\mathbb{Q})/2) \leq 4$, so $r = 0$.

References

[Kob] Koblitz, Neal. Introduction to elliptic curves and modular forms. Second edition. Graduate Texts in Mathematics, 97. Springer-Verlag, New York, 1993. Graduate Texts in Mathematics.

[SJ09] Silverman, Joseph H. The arithmetic of elliptic curves. Second edition. Graduate Texts in Mathematics, 106. Springer, Dordrecht, 2009.

[DJ07] David Cox, John Little, Donal O' Shea, Ideals, Varieties, and Algorithms,Third edition, 2007.

[ST92] Silverman, Joseph H.; Tate, John. Rational points on elliptic curves. Undergraduate Texts in Mathematics. Springer-Verlag, New York, 1992.

[SIA] Shafarevich, Igor R. Basic algebraic geometry. 2. Schemes and complex manifolds. Third edition. Translated from the 2007 third Russian edition by Miles Reid. Springer, Heidelberg, 2013.

[Ma77] B. Mazur, Modular curves and the Eisenstein ideal, Inst. Hautes Etudes Sci. Publ. Math. 47 (1977), 33-186.

[Me92] J-F. Mestre, Rang de courbes elliptiques d'invariant donn'e, C. R. Acad. Sci. Paris 314 (1992), 919-922.

[Me98] J-F. Mestre, Rang de certaines familles de courbes elliptiques d'invariant donn'e, C. R. Acad. Sci. Paris 327 (1998), 763-764.

[Me00] J-F. Mestre, Ranks of twists of elliptic curves, lecture at MSRI, September 11, 2000.

[R93] D. Rohrlich, Variation of the root number in families of elliptic curves, Compositio Math. 87 (1993), 119-151.

[RS01] K. Rubin, A. Silverberg, Rank frequencies for quadratic twists of elliptic curves, Exper. Math. 10 (2001), 559-569.

[S83] J. H. Silverman, Heights and the specialization map for families of abelian varieties, J. Reine Angew. Math. 342 (1983), 197-211.

[S86] J. H. Silverman, The arithmetic of elliptic curves, Graduate Texts in Mathematics 106, Springer-Verlag, New York, 1986.

[ST95] C. L. Stewart, J. Top, On ranks of twists of elliptic curves and powerfree values of binary forms, J. Amer. Math. Soc. 8 (1995), 943-973.

[CF86] J. W. S. Cassels and A. Frohlich (eds.), Algebraic number theory, London, Academic Press Inc.[Harcourt Brace Jovanovich Publishers], 1986, Reprint of the 1967 original.

[CS86] Gary Cornell and Joseph H. Silverman (eds.), Arithmetic geometry, Springer-Verlag, New York, 1986, Papers from the conference held at the University of Connecticut, Storrs, Connecticut, July 30-August 10, 1984.

[Mil86] J. S. Milne, Arithmetic duality theorems, Academic Press Inc., Boston, MA, 1986.

[PS99] Bjorn Poonen and Michael Stoll, The Cassels-Tate pairing on polarized abelian varieties, Ann. of Math. (2) 150 (1999), no. 3, 1109-1149.

[Ser79] Jean-Pierre Serre, Local fields, Springer-Verlag, New York, 1979, Translated from the French by Marvin Jay Greenberg.

[Ser97] Jean-Pierre Serre, Lectures on the Mordell-Weil theorem, third ed., Friedr. Vieweg & Sohn, Braunschweig, 1997, Translated from the French and edited by Martin Brown from notes by Michel Waldschmidt, With a foreword by Brown and Serre.

[Ser02] Jean-Pierre Serre, Galois cohomology, english ed., Springer-Verlag, Berlin, 2002, Translated from the French by Patrick Ion and revised by the author.