Indian Institute of Technology, Kanpur

Under Graduate Project-2019 Project Report
Rational points on Elliptic Curves

Submitted by
Ajay Prajapati
Roll No- 170063
Dept. of Mathematics and Statistics
Indian Institute of Technology, Kanpur

Under the guidance of
Somnath Jha
Dept. of Mathematics and Statistics
Indian Institute of Technology, Kanpur

ABSTRACT
This report is the culmination of a semester-long reading project on Elliptic curves under the guidance of Dr. Somnath Jha, IIT Kanpur. This is a report of what was learnt during course of the project starting from projective geometry, then defining elliptics curves, etc. The main focus of this project was on one of most celebrated results in theory of Elliptic curves, Mordell's Theorem.

Contents

1 Preliminaries

1.1 Introduction

The **theory of Diophantine equations** is that branch of number theory that deals with the solution of polynomial equations in either integers or rational numbers.

Here the degree of polynomial and no. of variables in polynomial can be anything.Rational and integer solutions of a n degree polynomial equation in one variable can be found easily. Then comes one degree equations in two variables. They represent lines in $\mathbb{R}^2$ and are easy to solve. Then two degree equations in two variables are conics. Rational and integer points on them have been fully understood. Then comes **cubic equation in two variables**. They were the main focus of this project as understanding rational and integer points on them is a lot harder than previous cases.

Before moving on we briefly look at above cases:

1) Polynomial Equation in one variable

$$a_0 + a_1x^1 + ... + a_nx^n = 0$$

where $a_i \in \mathbb{Z}$ $\forall$ i=1, 2,.... n

Gauss' lemma says that if p/q is a rational solution written in lowest terms, then q divides a_n and p divides a_0. This gives us a small list of possible rational solutions, and we can substitute each of them into the equation to determine the actual solutions.

2) Linear Equation in two variable

$$\text{ax + by + c = 0}$$

where a, b, c $\in \mathbb{Z}$. They represent a line in $\mathbb{R}^2$.

-Always infinitely many rational solutions

-No integer solutions if gcd(a, b) $\nmid$ c

-Infinitely integer solutions if gcd(a, b) $\mid$ c.

1.2 Rational Points on Conics

A point (x, y) is called **rational point** if x, y $\in \mathbb{Q}$.

A line ax+by+c=0 is called **rational line** if a, b, c $\in \mathbb{Q}$.

General form of conic: $ax^2 + bxy + cy^2 + dx + ey + f = 0$

A conic is **rational conic** if a, b, c, d, e, f $\in \mathbb{Q}$.

Given two rational points, the line through them is a rational line. Also, given two rational lines, the point of intersection is a rational point. But if a rational conic intersects with rational line, either both points are rational or both are not rational. This is because by substituting y from line to conic, a quadratic equation in x is obtained whose coefficients are rational. Thus given that one point of intersection is rational then so is the other. This gives simple algorithm to determine all rational points on conic:

Step 1: Find a rational point O on the given rational conic

Step 2: We just draw some rational line and project the conic onto the line from the

point O(To project O itself onto the line, use the tangent line O)
It's easy to see that there is one-to-one correspondence between the rational points on conic and the rational points on line.

1.3 Projective Geometry and the Projective Plane

Define an equivalence relation $\sim$ on $\mathbb{R}^3 \setminus \{(0,0,0)\}$ as:
(a,b,c) $\sim$ (a',b',c') iff $a = ta', b = tb', c = tc'$ for some non-zero t.

Definition 1.1. The **projective plane** $\mathbb{P}^2$ is defined to be set of all equivalence classes under $\sim$.

Definition 1.2. An equivalence class of (a, b, c) is represented as [a, b, c] and a, b, c are called **homogenous coordinates** of [a, b, c].

Definition 1.3. A **line** in $\mathbb{P}^2$ to be the set of points [a, b, c] $\in \mathbb{P}^2$ whose coordinates satisfy an equation of the form

$$\alpha\text{X} + \beta\text{Y} + \gamma\text{Z} = 0$$

for some constants α, β, γ not all zero.

Definition 1.4. A polynomial F(X,Y,Z) is called a **homogeneous polynomial of degree d** if it satisfies the identity

$$F(tX, tY, tZ) = t^d F(X, Y, Z) \tag{1}$$

Definition 1.5. A **projective curve** C in the projective plane $\mathbb{P}^2$ to be the set of solutions to the equation

$$C : F(X, Y, Z) = 0 \tag{2}$$

where F is a non-constant homogeneous polynomial.

1.4 Intersections of Projective Curves

Definition 1.6. Let K be a field. Two curves C_1 : f(x, y)=0 and C_2 : g(x, y)=0 where f, g $\in$ K[x, y] are said to have **no common components** if gcd(f, g) $\in$ K.(K[x, y] is a UFD, hence gcd is well defined)

Definition 1.7. To each point P $\in \mathbb{P}^2$ assign a **multiplicity or intersection index** $I(C_1 \cap C_2, P)$. This is a non-negative integer reflecting the extent to which C_1 and C_2 are tangent to one another at P or are not smooth at P.

Theorem 1.8. ***(Bezout's Theorem)*** *Let C_1 and C_2 be projective curves with no common components. Then*

$$\sum_{P \in C_1 \cap C_2} I(C_1 \cap C_2, P) = (degC_1)(degC_2) \tag{3}$$

where the sum is over all points of $C_1 \cap C_2$ having complex coordinates. In particular, if C_1 and C_2 are smooth curves with only transversal intersections, then $(C_1 \cap C_2)$ = (deg C_1)(deg C_2), and in all cases there is an inequality

$$(C_1 \cap C_2) \leq (degC_1)(degC_2). \tag{4}$$

Theorem 1.9. ***Cubic Cayley–Bacharach Theorem*** *Let C_1 and C_2 be cubic curves in $\mathbb{P}^2$ without common components, and assume that C_1 is smooth. Suppose that D is another cubic curve that contains eight of the intersection points of $C_1 \cap C_2$ counting multiplicities i.e.*
if $C_1 \cap C_2 = \{P1, \ . \ . \ . \ , Pr\}$, then

$$I(C_1 \cap D, P_i) \geq I(C_1 \cap C_2, P_i) \text{ for } 1 \leq i \leq r,$$

and

$$I(C_1 \cap D, P_r) \geq I(C_1 \cap C_2, P_r) \text{ - } 1$$

Then D goes through the ninth point of $C_1 \cap C_2$ i.e.

$$I(C_1 \cap D, P_r) \geq I(C_1 \cap C_2, P_r)$$

2 Solving Cubic Equation

2.1 Group law on General Cubic

From now on, we view a curve on projective plane $\mathbb{P}^2$ because we want Bezout's theorem to hold which is not true when we view a curve in euclidean plane $\mathbb{R}^2$.
Given any two rational points P and Q on a rational cubic, draw the line joining P to Q and obtain a third rational point and denote it by P$\star$Q.
Given a fixed rational point O on cubic, define law of composition "+" on the set of all rational points on the cubic as:
P+Q = O$\star$(P$\star$Q)

The properties of "+" operation are:
1) Commutative: P+Q=Q+P
2) O is identity element (by definition)
3) Let S = O $\star$ O. Then for any point Q, -Q = Q $\star$ S
4) Associative: (P + Q) + R = P + (Q + R)

This makes the set of all rational points on cubic into a **group**.
Remark 2.1. Checking that (1), (2) and (3) are true is easy but checking associativity is surprisingly hard and this is where Theorem 1.9 is used.

2.2 Weierstrass Normal Form

General cubic is given by,

$$ax^3 + bx^2y + cxy^2 + dy^3 + ex^2 + fy^2 + gxy + hx + iy + j = 0 \tag{5}$$

We can transform this equation into much simpler equation of form

$$y^2 = 4x^3 - g_2x - g_3 \tag{6}$$
$$y^2 = x^3 + ax^2 + bx + c \tag{7}$$

Definition 2.2. Equations of either of the above form are known as **Weierstrass form**.

Studying general cubic is equivalent to studying Weierstrass form because equations (1), (2) and (3) are birationally equivalent to each other.

Definition 2.3. Let $f(x) = x^3 + ax^2 + bx + c$ be the right part of equation (3). If f(x) has distinct roots in $\mathbb{C}$ then the cubic $y^2 - f(x) = 0$ is known as **non-singular cubic**(meaning tangent is defined at any point on cubic).

Definition 2.4. Non-singular cubics of above form are known as **elliptic curve**.

Singular cubics are easier to deal with and generally behave like conics. Hence finding rational or integer points on them is easy. From now onwards, we only focus on non-singular cubics.

2.3 Group Law on Elliptic Curves

Given a non-singular cubic,

$$y^2 = f(x) = 4x^3 - g_2 x - g_3 \tag{8}$$

make it homogeneous by setting x = X/Z and y = Y/Z

$$Y^2 Z = X^3 + aX^2 Z + bXZ^2 + cZ^3 \tag{9}$$

Substituting Z = 0 into the equation gives $X^3 = 0$, which has a triple root X = 0. This means that the cubic meets the line at infinity in three points, but the three points are all the same! So a cubic has exactly one point at infinity, namely the point at infinity where vertical lines (that is, lines x = constant) meet. Call that point O and define it to be a rational point. Take it as the identity element when making the set of rational points on curve into a group.

Explicit formulas for group law are:
1) If Q = (x, y), then -Q = (x, -y)
2) If $P_1 = (x_1, y_1)$, $P_2 = (x_2, y_2)$ and let $P_1 \star P_2 = (x_3, y_3)$ then

$$P_1 + P_2 = (x_3, -y_3) \text{ where} \tag{10}$$

$$x_3 = \lambda^2 - a - x_1 - x_2 \text{ and } y_3 = \lambda x_3 + \nu \tag{11}$$

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1} \text{ and } \nu = y_1 - \lambda x_1 \tag{12}$$

To add a point P to itself(i.e. finding 2P), take the line for finding $P \star P$ to be the tangent line drawn at P.
Since y^2=f(x), and λ is the slope of the line joining P_1 and P_2 hence when $P_1 = P_2$ we have λ=$\frac{f'(x)}{2y}$.
Substituting this in equations (8) and (9)

$$\text{x-coordinate of 2(x, y)} = \frac{x^4 - 2bx^2 - 8cx + b^2 - 4ac}{4x^3 + 4ax^2 + 4bx + 4c} \tag{13}$$

This formula for x(2P) is called the **duplication formula**.

3 Points of Finite Order

3.1 Points of Order Two and Three

Theorem 3.1. ***(Points of Order Two and Three)*** *Let C be a non-singular cubic curve*

$$C : y^2 = f(x) = x^3 + ax^2 + bx + c. \tag{14}$$

(a) A point P = (x, y) = O on C has order two if and only if y = 0.
(b) The curve C has exactly four points of order dividing two. These four points form a group that is a product of two cyclic groups of order two.
(c) A point P = (x, y) = O on C has order three if and only if x is a root of the polynomial

$$\psi^3(x) = 3x^4 + 4ax^3 + 6bx^2 + 12cx + 4ac - b^2. \tag{15}$$

(d) The curve C has exactly nine points of order dividing three. These nine points form a group that is a product of two cyclic groups of order three.

3.2 The Nagell–Lutz Theorem

Let C be a non-singular elliptic curve

$$C(\mathbb{Q}) = \{(x, y) \in C : x, y \in \mathbb{Q}\} \cup \{O\}. \tag{16}$$

If C is given by the equation

$$y^2 = f(x) = x^3 + ax^2 + bx + c \tag{17}$$

where a, b, c $\in \mathbb{Z}$.

Then the quantity

$$D = -4a^3c + a^2b^2 + 18abc - 4b^3 - 27c^2 \tag{18}$$

is called **discriminant** of f(x).

The discriminant is non-zero if and only if cubic is non-singular.

Lemma 3.2. *Let P = (x, y) be a point on above cubic curve C such that both P and 2P have integer coordinates. Then either y = 0 or $y|D$.*

Proof. Assume y $\neq$ 0. Hence 2P $\neq$ O. So write 2P=(X, Y). By assumption x, y, X, Y $\in \mathbb{Z}$.By duplication formula,

$$2x + X = \lambda^2 - a, \text{ where } \lambda = \frac{f'(x)}{2y} \tag{19}$$

. Since x, X, a $\in \mathbb{Z}$ and $\lambda \in \mathbb{Q} \Rightarrow \lambda \in \mathbb{Z}$.
But y, $f'(x) \in \mathbb{Z} \Rightarrow y|f'(x)$
Also y^2 = f(x) $\Rightarrow y|f(x)$.
$D = -4a^3c + a^2b^2 + 18abc - 4b^3 - 27c^2$
$= ((18b - 6a^2)x - (4a^3 - 15ab + 27c))f(x) + ((2a^2 - 6b)x^2 + (2a^3 - 7ab + 9c)x + (a^2b + 3ac - 4b^2))f'(x)$
$= r(x)f(x) + s(x)f'(x)$.
Here r(x), s(x) $\in \mathbb{Z}[x]$ hence $y|D$. □

Let p be a prime. Then **order** of a rational number(w.r.t prime p) is defined as (ord(O) = ∞)

$$ord(\frac{m}{n}p^{\nu}) = \nu \text{ where } p \nmid m \text{ and } p \nmid n \tag{20}$$

Let R_p be the ring of rational numbers with denominator prime to p i.e.

$$R_p = \{\frac{x}{y} \in \mathbb{Q} | x, y \in \mathbb{Z}, gcd(y, p) = 1\} \tag{21}$$

$$R_p = \{q \in \mathbb{Q} | ord(q) \geq 0\} \tag{22}$$

$$C(p^{\nu}) = \{(x, y) \in C(\mathbb{Q}) : ord(x) \leq -2\nu\} \cup \{O\} \tag{23}$$

Proposition 3.3. *Let p be a prime, R_p and $C(p^{\nu})$ as above.*
(a) C(p) consists of all rational points (x, y) for which the denominator of either x or y is divisible by p.
(b) For every $\nu \geq 1$, the set $C(p^{\nu})$ is a subgroup of C($\mathbb{Q}$).
(c) The map

$$\frac{C(p^{\nu})}{C(p^{3\nu})} \to \frac{p^{\nu}R_p}{p^{3\nu}R_p}, P = (x, y) \longmapsto \frac{x}{y}, \tag{24}$$

is a one-to-one homomorphism.(By convention, $O \longmapsto$ 0.)

Proof. a) Suppose (x, y) $\in C(\mathbb{Q})$ and $p|deno(x)$. Thus

$$x = \frac{m}{np^{\mu}} \text{ and } y = \frac{u}{vp^{\sigma}} \tag{25}$$

where $\mu > 0$ and $p \nmid m, n, u, v$.
Substituting x and y in above equation, we get
$2\sigma = 3\mu$. $\Rightarrow 2|\mu$ and $3|\sigma$ i.e. $\mu = 2\nu$ and $\sigma = 3\nu$.
Similary if $\sigma > 0$ then again $\mu = 2\nu$ and $\sigma = 3\nu$.

b)Make change of coordinates from (x, y) to (s, t)

$$t = \frac{x}{y} \text{ and } s = \frac{1}{y} \tag{26}$$

Then $y^2 = x^3 + ax^2 + bx + c$ becomes

$$s = t^3 + at^2s + bts^2 + cs^3 \tag{27}$$

Clearly, the transformation is invertible. Zero element O of(x, y)-plane becomes (0, 0) in (t,s)-plane and all points except points of order 2(y=0) are there in (t, s)-plane. A line $y = \lambda x + \nu$ becomes a line (t, s)-plane

$$s = -\frac{\lambda}{\nu}t + \frac{1}{\nu} \tag{28}$$

Now, let P=(x, y) $\in$ C(p) in x-y plane, then

$$x = \frac{m}{np^{2(\nu+i)}} \text{ and } y = \frac{u}{wp^{3(\nu+i)}} \tag{29}$$

$$t = \frac{x}{y} = \frac{mw}{nu} p^{\nu+i} \text{ and } s = \frac{1}{y} = \frac{w}{u} p^{3(\nu+i)} \tag{30}$$

Hence, point (t, s) $\in C(p^\nu)$ iff t $\in p^\nu R_p$ and s $\in p^{3\nu} R_p$. Now, to prove C(p^ν) a subgroup, need to show that if $P_1, P_2 \in$ C(p^ν) then $P_1 + P_2 \in C(p^\nu)$.Let $P_1 = (t_1, s_1)$ and $P_2 = (t_2, s_2)$ be distinct points in C(p$^\nu$).

If $t_1 = t_2$ then letting $P_1 \star P_2 = (t_1, s_3)$ gives $P_1 + P_2 = (-t_1, -s_3)$. Since $t(P_1 + P_2) \in p^\nu R_p \implies P_1 + P_2 \in p^\nu R_p$. If $t_1 \neq t_2$ then let $s = \alpha t + \beta$ be line passing through them then $\alpha = (s_2 - s_1)/(t_2 - t_1)$. Also, they lies on the curve with equation (26), hence after some computation, we get

$$\alpha = \frac{s_2 - s_1}{t_2 - t_1} = \frac{t_2^2 + t_1 t_2 + t_1^2 + a(t_2 + t_1)s_2 + bs_2^2}{1 - at_1^2 - bt_1(s_2 + s_1) - c(s_2^2 + s_1 s_2 + s_1^2)} \tag{31}$$

If $P_1 = P_2$ then

$$\alpha = \frac{ds}{dt}(P) = \frac{at_1^2 + 3at_1 s_1 + bs_1^2}{1 - at_1^2 - 2bt_1 s_1 - 3cs_1^2} \tag{32}$$

Note that (31) is just (30) substituted with $t_1 = t_2 and s_1 = s_2$ hence (30) is valid in all cases. Substitute the equation of line in (26) to obtain a cubic equation. If $P_1 \star P_2 = P_3 = (t_3, s_3)$ then

$$t_1 + t_2 + t_3 = -\frac{\alpha\beta + 2b\alpha\beta + 3c\alpha^2\beta}{1 + a\alpha + b\alpha^2 + c\alpha^3} \tag{33}$$

To find $P_1 + P_2$ join points $P_1 \star P_2$ and (0, 0) and third point of intersection is required point. (26) is symmetric about origin hence, $P_1 + P_2 = (-t_3, -s_3)$.

In (30), numerator $\in p^{2\nu} R_p$ and quantity $-at_1^2 - bt_1(s_2 + s_1) - c(s_2^2 + s_1 s_2 + s_1^2)$ also lies in $p^{2\nu} R_p$. Hence denominator is unit in $R_p \implies \alpha \in p^{2\nu} R_p$. Since $\beta = s_1 - \alpha t_1$ and from above we get $\beta \in p^{3\nu} R_p$. (since $t_1, t_2 \in p^\nu R_p$ and $s_1, s_2 \in p^{3\nu} R_p$)

Observe in (32) numerator $\in p^{3\nu} R_p$ and denominator is a unit in R_p. Hence $t_1 + t_2 + t_3 \in p^{3\nu} R_p$. In particular, $t_3 \in p^\nu R_p \implies t(P_1 + P_2) \in p^\nu R_p \implies P_1 + P_2 \in C(p^\nu)$. Also if P=(t, s) $\in C(p^\nu)$ then -P=(-t, -s) $\in C(p^\nu)$.

Hence $C(p^\nu)$ is a subgroup.

c) Observe that above we have proven something bit stronger.

$$t(P_1) + t(P_2) - t(P_1 + P_2) \in p^{3\nu} R_p \forall P_1, P_2 \in C(p^\nu) \tag{34}$$

where t(P) denotes t coordinate of P i.e. t(P)=x(P)/y(P). Equation (33) can be written other form as

$$t(P_1 + P_2) \equiv t(P_1) + t(P_2)(mod p^{3\nu} R_p) \tag{35}$$

Hence then map $C(p^\nu) \longrightarrow \frac{p^\nu R_p}{p^{3\nu} R_p}$ is actually a well defined homomorphism. The kernel of this homomorphism consists of all points P with t(P) $\in p^{3\nu} R_p$ i.e. P $\in C(p^{3\nu})$. So by first isomorphism theorem, we get one-to-one homomorphism as claimed in theorem. □

Theorem 3.4. ***(Nagell–Lutz Theorem)*** *Let $y^2 = f(x) = x^3 + ax^2 + bx + c$ be a non-singular cubic curve with integer coefficients a, b, c, and let D be the discriminant of f(x). Let P = (x, y) be a rational point of finite order. Then x and y are integers, and either y = 0, in which case P has order two, or else y divides D.*

Proof. Let P=(x, y) $\in C(\mathbb{Q})$ be a point of finite order m with m $\geq$ 2. Let P $\in$ C(p) for some prime p. Then $\exists$ some $\nu > 0$ s.t. P $\in C(p^{\nu})$ but P $\notin C(p^{\nu+1})$ ($\nu =$ -$\frac{1}{2}$ord(x)).
If $p \nmid m$ then repeated application of () gives

$$t(mP) \equiv mt(P) \text{ (mod } p^{3\nu}R_p) \tag{36}$$

But t(mP)=t(O)=0 and gcd(p, m)=1 gives

$$0 \equiv t(P) \text{ (mod } p^{3\nu}R_p) \tag{37}$$

This means P $\in C(p^{3\nu})$ contradicting P $\notin C(p^{\nu+1})$.
If $p|m$ then m=p^{λ} n where $\lambda > 0$ and gcd(p, n)=1.
Since C(p) is a subgroup, let Q=p^{λ}P then Q $\in C(p)$ and $nQ = O$. Apply above to Q to again arrive at contradiction.
Hence any point with finite order has integer coordinates.
Let P=(x, y) has finite order then 2P also has finite order hence P and 2P both has integer coordinates. Then by lemma 4.1 y=0 or $y|D$.

□

4 The Group of Rational Points

4.1 Descent

Theorem 4.1. ***(Desecent Theorem)*** *Let* Γ *be a commutative group, and there is a function* $h : \Gamma \longrightarrow [0, \infty)$ *with following properties:*
(a)$\forall M \in \mathbb{R}$*, the following set is finite.*

$$\{P \in \Gamma : h(P) \leq M\} \tag{38}$$

(b) For every $P_0 \in \Gamma$, $\exists \kappa_0$ *such that*

$$h(P + P_0) \leq 2h(P) + \kappa_0 \;\forall\; P \in \Gamma. \tag{39}$$

(c) $\exists \kappa$ *such that*

$$h(2P) \geq 4h(P) - \kappa \;\forall\; P \in \Gamma. \tag{40}$$

(d) The subgroup Γ*:2*Γ *is finite.*
Then Γ *is finitely generated.*

Proof. Let $Q_1, Q_2, ...Q_n$ be cosets representatives of 2Γ in Γ. Let P be any element in Γ, then $\exists$ indices $i_1, i_2, ...i_m$ and elements $P_1, P_2, ..., P_m \in \Gamma$ such that

$$P = Q_{i_1} + 2P_1 \tag{41}$$

$$P_1 = Q_{i_2} + 2P_2 \tag{42}$$

$$\vdots$$

$$P_{m-1} = Q_{i_m} + 2P_m \tag{43}$$

Substitute values of $P_1, P_2, ...P_{m-1}$ in (30) to get

$$P = Q_{i_1} + 2Q_{i_2} + 4Q_{i_3} + ... + 2^{m-1}Qi_n + 2^m P_m \tag{44}$$

Apply (b) part to $-Q_i$ to obtain constants κ_i so that

$$h(P - Q_i) \leq 2h(P) + \kappa_i \; \forall \; P \in \Gamma. \tag{45}$$

Let $\kappa' = max\{\kappa_1, \kappa_2, ...\}$. This κ' is well defined because $Q_i's$ are finite.Hence,

$$h(P - Q_i) \leq 2h(P) + \kappa' \; \forall \; P \in \Gamma. \tag{46}$$

Let κ be constant from (c). Then

$$\begin{aligned} 4h(P_j) &\leq h(2P_j) + \kappa \\ &= h(P_{j-1} - Qi_j + \kappa \\ &\leq 2h(P_{j-1}) + \kappa' + \kappa \end{aligned} \tag{47}$$

$$\begin{aligned} h(P_j) &\leq \frac{1}{2}h(P_{j-1}) + \frac{1}{4}(\kappa' + \kappa) \\ &= \frac{3}{4}h(P_{j-1}) + \frac{1}{4}(\kappa' + \kappa - h(P_{j-1})) \end{aligned} \tag{48}$$

Hence if $\kappa' + \kappa \leq h(P_{j-1})$, then

$$h(P_j) \leq \frac{3}{4}h(P_{j-1}) \tag{49}$$

Hence, start with any P $\in \Gamma$ and find sequence of points $P_1, P_2, ...$ as described before then height keeps on decreasing as long as $h(P_{j-1}) \geq \kappa' + \kappa$. Eventually $\exists$ index m s.t. $h(P_m) \leq \kappa' + \kappa$.

Therefore any P $\in \Gamma$ can be written as

$$P = a_1 Q_1 + a_2 Q_2 + ... + a_n Q_n + 2^m R \tag{50}$$

where $a_1, a_2, ...a_n \in \mathbb{Z}$ and h(R) $\leq \kappa' + \kappa$. Hence, the set

$$\{Q_1, Q_2, ...Q_n\} \cup \{P \in \Gamma : h(P) \leq \kappa' + \kappa\} \tag{51}$$

generates Γ which is finite by (a) and (d). □

4.2 Mordell's Theorem

Definition 4.2. Let x = m/n $\in \mathbb{Q}$ where gcd(m, n)=1.Then *height of x* is defined as

$$H(x) = H(\frac{m}{n}) = max\{|m|, |n|\} \tag{52}$$

Definition 4.3. Let P=(x, y) $\in C(\mathbb{Q})$ then *height H of P* and *small height h of P* are defined as

$$H(P) = H(x) \tag{53}$$

$$h(P) = logH(P) \tag{54}$$

Lemma 4.4. *$\forall M \in \mathbb{R}$, the following set is finite.*

$$\{P \in C(\mathbb{Q}) : h(P) \leq M\} \tag{55}$$

Proof. x(P) $\leq e^M \Rightarrow$ finitely many possiblities for x(P)
$\Rightarrow$ finitely many possiblities for y(P)
$\Rightarrow$ finitely many possiblities for P. □

Lemma 4.5. *Let $P_0 \in C(\mathbb{Q})$. $\exists$ constant κ_0 that depends on P_0 and on a, b, and c, so that*

$$h(P + P_0) \leq 2h(P) + \kappa_0 \ \forall \ P \in C(\mathbb{Q}). \tag{56}$$

Remark 4.6. If P=(x, y) $\in C(\mathbb{Q})$ then x and y have form

$$x = \frac{m}{e^2} \text{ and } y = \frac{n}{e^3} \tag{57}$$

where gcd(m, e)=gcd(n, e)=1. (By proof of Propostion 4.2)

Remark 4.7. If P=($\frac{m}{e^2}, y = \frac{n}{e^3}$), then
$|m| \leq$ H(P) and $e^2 \leq$ H(P).
Substitute P in curve equation to obtain

$$n^2 = m^3 + ae^2m^2 + be^4m + ce^6 \tag{58}$$

Use triangle inequality to obtain

$$\begin{aligned} |n^2| &\leq |m^3| + |ae^2m^2| + |be^4m| + |ce^6| \\ &\leq H(P)^3 + |a|H(P)^3 + |b|H(P)^3 + |c|H(P)^3 \end{aligned} \tag{59}$$

Take K=$\sqrt{(1 + |a| + |b| + |c|)}$ to obtain

$$|n| \leq KH(P)^{3/2} \tag{60}$$

Proof. In proving existence of κ_0, it is sufficient to prove inequality for all P except finitely many points.
Let P $\in C(\mathbb{Q}) \setminus \{P_0, -P_0, O\}$ Let P=(x, y) and $P + P_0 = (\xi, \eta)$. Then use equations (8) and (9) to obtain

$$\begin{aligned} \xi &= \frac{(y - y_0)^2}{(x - x_0)^2} - a - x - x_0 \\ &= \frac{(y - y_0)^2 - (x - x_0)^2(x + x_0 + a)}{(x - x_0)^2} \end{aligned} \tag{61}$$

Substitute $y^2 - x^3 = ax^2 + bx + c$ in numerator to obtain

$$\xi = \frac{Ay + Bx^2 + Cx + D}{Ex^2 + Fx + G} \tag{62}$$

where A, B,....,G $\in \mathbb{Z}$ and depends on a, b, c and (x_0, y_0). Substitute P=($\frac{m}{e^2}, y = \frac{n}{e^3}$) to obtain

$$\xi = \frac{Ane + Bm^2 + Cme^2 + De^4}{Em^2 + Fme^2 + Ge^4} \tag{63}$$

$$H(\xi) \leq max\{|Ane + Bm^2 + Cme^2 + De^4|, |Em^2 + Fme^2 + Ge^4|\} \qquad (64)$$

Use Remark 5.7 and triangle inequality to obtain bound on two expression and get

$$H(P + P_0) = H(\xi) \leq max\{|AK| + |B| + |C| + |D|, |E| + |F| + |G|\}H(P)^2 \quad (65)$$

Take log both sides to obtain the required inequality. □

Lemma 4.8. *Let $\phi(X)$ and $\psi(X) \in \mathbb{Z}[X]$ and $gcd(\phi(X), \psi(X))=1$ in $\mathbb{C}[X]$.Let $d=max\{deg(f), deg(g)\}$, then*
(a) $\exists R \in \mathbb{Z}$, that depends on $\phi(X)$ and $\psi(X)$, so that

$$gcd(n^d\phi(\frac{m}{n}), n^d\psi(\frac{m}{n}))|R \;\forall\; \frac{m}{n} \in \mathbb{Q} \qquad (66)$$

(b) $\exists$ a constant κ_1, depending on ϕ and ψ, so that $\forall\frac{m}{n} \in \mathbb{Q}$ that are not roots of ψ,

$$dh(\frac{m}{n}) - \kappa_1 \leq h(\frac{\phi(m/n)}{\psi(m/n)}) \qquad (67)$$

Proof. a) Observe that $n^d\phi(\frac{m}{n})$ and $n^d\psi(\frac{m}{n})$ are both integers. Hence gcd is well defined. WLOG, let deg(ϕ)=d and deg(ψ)=e $\leq$. Let

$$\Phi(m, n) = n^d\phi(\frac{m}{n}) = a_0m^d + a_1m^{d-1}n + ... + a_dn^d, \qquad (68)$$

$$\Psi(m, n) = n^d\psi(\frac{m}{n}) = b_0m^en^{d-e} + b_1m^{e-1}n^{d-e+1} + ... + b_en^d. \qquad (69)$$

and let γ=$gcd(\Phi(m, n), \Psi(m, n))$. Since $gcd(\phi(X), \psi(X)) = 1$ in $\mathbb{Q}$[X], $\exists$ F(X) and G(X) $\in \mathbb{Q}[X]$ s.t.

$$F(X)\phi(X) + G(X)\psi(X) = 1 \qquad (70)$$

Take A be a large enough constant s.t. AF(X) and AG(X) $\in \mathbb{Z}[X]$ and D=max$\{deg(F), deg(G)\}$

Evaluate (61) at $X = \frac{m}{n}$ and multiply both sides by $An^(D + d)$ to obtain

$$n^DAF(\frac{m}{n})\Phi(\frac{m}{n}) + n^DG(\frac{m}{n})\Psi(\frac{m}{n}) = An^{D+d} \qquad (71)$$

Hence $\gamma|An^{D+d}$
Also $\gamma|\Phi(m, n) \Rightarrow \gamma|An^{D+d-1}\Phi(m, n)$

$$An^{D+d-1}\Phi(m, n) = Aa_0m^dn^{D+d-1} + Aa_1m^{d-1}n^{D+d} + ... + Aa_dn^{D+2d-1}. \qquad (72)$$

$\Rightarrow \gamma|Aa_0m^dn^{D+d-1} \Rightarrow \gamma|gcd(Aa_0m^dn^{D+d-1}, An^{D+d})$
hence $\gamma|Aa_0n^{D+d-1}$.
Repeating this argument D+d times, we get that $\gamma|Aa_0^{D+d}$ which is independent of m and n.

b)There are finitely many rational which are roots of ψ and hence it is sufficient to prove the inequality ignoring them.Now,

$$\xi = \frac{\phi(m/n)}{\psi(m/n)} = \frac{\Phi(m, n)}{\Psi(m, n)} \qquad (73)$$

Now, use result from (a) to get

$$\begin{aligned} H(\xi) &\geq \frac{1}{R} max\{|\Phi(m,n)|, |\Psi(m,n)|\} \\ &\geq \frac{1}{2R}(|\Phi(m,n)| + |\Psi(m,n)|) \end{aligned} \tag{74}$$

Now, $H(\frac{m}{n})^d = max(|m|^d, |n|^d)$ and consider

$$\begin{aligned} \frac{H(\xi)}{H(m/n)^d} &\geq \frac{1}{2R}\frac{(|n^d\phi(\frac{m}{n})|, |n^d\psi(\frac{m}{n})|)}{max\{|m|^d, |n|^d\}} \\ &\geq \frac{1}{2R}\frac{(|\phi(\frac{m}{n})| + |\psi(\frac{m}{n})|)}{max\{|\frac{m}{n}|^d, 1\}} \end{aligned} \tag{75}$$

In the real valued function

$$p(t) = \frac{(|\phi(t)| + |\psi(t)|)}{max\{|t|^d, 1\}} \tag{76}$$

the deg(num(p))=deg(deno(p)) hence p(t) is bounded outside a compact set(since limit is finite as t approaches ∞).Since p(t) is continuous, inside a compact set its maxima and minima exists. Also the function is non-zero since $gcd(\phi(X), \psi(X)) = 1$ hence $\exists$ constant C $>$ 0 s.t. $p(t) > C \ \forall t \in \mathbb{R}$. Hence,

$$H(\xi) \geq \frac{C}{2R}H(\frac{m}{n})^d \tag{77}$$

take logarithm both sides to get the desired result. □

Lemma 4.9. *$\exists$ constant κ, depending on a, b, and c, so that*

$$h(2P) \geq 4h(P) - \kappa \ \forall \ P \in C(\mathbb{Q}). \tag{78}$$

Proof. Let P=(x, y) and 2P=(ξ, η). By (8), (9) and (10),

$$\begin{aligned} \xi &= \frac{(f'(x))^2 - (8x + 4a)f(x)}{4f(x)} \\ &= \frac{x^4 - 2bx^2 - 8cx + b^2 - 4ac}{4x^3 + 4ax^2 + 4bx + 4c} \end{aligned} \tag{79}$$

Since gcd($f'(x)$, f(x))=1 in $\mathbb{C}[x] \Rightarrow$ gcd($num(\xi), deno(\xi)$)=1 in $\mathbb{C}[x]$. So apply first part of inequality of lemma 5.8(b) to get desired result. □

Proposition 4.10. *Let C and C be elliptic curves given by the equations*

$$C : y^2 = x^3 + ax^2 + bx \ and \ C : y^2 = x^3 + \overline{a}x^2 + \overline{b}x \tag{80}$$

where $\overline{a}$ = -2a and $\overline{b}$ = a^2 - 4b. Let T = (0, 0) $\in$ C
(a) There is a homomorphism $\phi : C \rightarrow \overline{C}$ defined by

$$\phi(P) = \begin{cases} (\frac{y^2}{x^2}, \frac{y(x^2-b)}{x^2}) \ if \ P = (x,y) \neq T, O \\ \overline{O} \ if \ P = T, O \end{cases} \tag{81}$$

The kernel of ϕ is $\{O, T\}$.
(b) Applying the same process to $\overline{C}$ gives a map $\overline{\phi} : \overline{C} \to \overline{\overline{C}}$. The curve $\overline{\overline{C}}$ is isomorphic to C via the map (x, y) $\mapsto$ $(\frac{1}{4}x, \frac{1}{8}y)$. There is thus a homomorphism $\psi : \overline{C} \to C$ defined by

$$\psi(\overline{P}) = \begin{cases} (\frac{\overline{y}^2}{4\overline{x}^2}, \frac{\overline{y}(\overline{x}^2-\overline{b})}{8\overline{x}^2}) \textit{ if } \overline{P} = (\overline{x},\overline{y}) \neq \overline{T},\overline{O} \\ O \textit{ if } \overline{P} = \overline{T},\overline{O} \end{cases} \tag{82}$$

(c) The composition $\psi \circ \phi : C \to C$ is the multiplication by two map,

$$\psi \circ \phi(P) = 2P \tag{83}$$

Proof. a) It can be easily checked that map ϕ is well-defined. The kernel of ϕ is obvious once it is proved to be homomorphism i.e.

$$\phi(P_1 + P_2) = \phi(P_1) + \phi(P_2) \;\forall\; P_1, P_2 \in C \tag{84}$$

When P_1 or P_2 is O, there is nothing to prove.When both P_1 and P_2 is T then formula can be easily verified. When one of P_1 or P_2 is T then also formula can be easily checked.
It suffices to show that if $P_1 + P_2 + P_3 =$ O, then $\phi(P_1) + \phi(P_2) + \phi(P_3) =$ O where none of the points $P_1, P_2, or P_3$ is equal to O or T.
If $P_1 + P_2 + P_3 =$ O, then P_1, P_2, P_3 are collinear. Let y = λx + ν be the line through them.(If two or three of them coincide, then the line should be appropriately tangent to the curve). Then $\nu \neq 0$. We must show that $\phi(P_1), \phi(P_2), and \phi(P_3)$ are the intersection of some line with $\overline{C}$. Take that line to be

$$y = \overline{\lambda}x + \overline{\nu} \text{ where } \overline{\lambda} = \frac{\nu\lambda - b}{\nu} \text{ and } \overline{\nu} = \frac{\nu^2 - a\nu\lambda + b\lambda^2}{\nu} \tag{85}$$

It is easy to check that $\phi(P_1), \phi(P_2), and \phi(P_3)$ lies on above line. Or check that that $\overline{x}(P_a 1), \overline{x}(P_2), \overline{x}(P_3)$ are the three roots of the cubic $(\overline{\lambda}x + \overline{\nu})^2 = \overline{f}(x)$.

b) The curve $\overline{\overline{C}}$ is given by the equation

$$\overline{\overline{C}} : y^2 = x^3 + 4ax^2 + 16bx \tag{86}$$

Also, it is easy to check that the map (x, y) $\mapsto$ (x/4, y/8) is an isomorphism.From (a), there is a homomorphism $\overline{\phi} : \overline{C} \to \overline{\overline{C}}$. Since the map ψ : $\overline{C} \to$ C is the composition of $\overline{\phi} : \overline{C} \to \overline{\overline{C}}$ with the isomorphism $\overline{\overline{C}} \to C$, it is clear that ψ is a well-defined homomorphism from $\overline{C}$ to C.

c) Now,

$$\phi(P) = (\frac{y^2}{x^2}, \frac{y(x^2-b)}{x^2}) \text{ and } \psi(\overline{x}, \overline{y}) = (\frac{\overline{y}^2}{4\overline{x}^2}, \frac{\overline{y}(\overline{x}^2-b)}{8\overline{x}^2}) \tag{87}$$

$$2P = 2(x, y) = (\frac{(x^2-y)^2}{4y^2}, \frac{(x^2-b)(x^4+2ax^3+6bx^2+2abx+b^2)}{8y^3}) \tag{88}$$

Using above equations, one can check that $\psi \circ \phi(x, y) = 2(x, y)$. One also needs to check if x=0 or y=0 then $\psi \circ \phi(P) = O$ since above formulas would not be valid in that case.

Also one can check by explicit calculations that $\overline{\phi} \circ \overline{\psi}(\overline{x}, \overline{y}) = 2(\overline{x}, \overline{y})$ or argue as follows: Since ϕ is homomorphism, $\phi(2P) = 2\phi(P)$. Also 2P=$\psi \circ \phi(P)$. Hence,

$$\phi \circ \psi(\phi(P)) = 2\phi(P) \tag{89}$$

Now $\phi : C \to \overline{C}$ is onto as a map of complex points, so for any $\overline{P} \in \overline{C}$ we can find a point P $\in$ C with $\phi(P) = \overline{P}$. Therefore $\phi \circ \psi(\overline{P}) = 2\overline{P}$(continuity argument). □

Lemma 4.11. *Let C, $\overline{C}, \phi$ and ψ are as in Proposition 4.10 and let Γ be group of rational points on C and similarly $\overline{\Gamma}$ is group of rational points on $\overline{C}$. Then,*
a) $\overline{O} \in \phi(\Gamma)$
b) $\overline{T}$ = (0, 0) $\in \phi(\Gamma)$ if and only if $\overline{b} = a^2 - 4b$ is a perfect square
c) Let $\overline{P} = (\overline{x}, \overline{y}) \in \overline{\Gamma}$ with $\overline{x} \neq 0$. Then $\overline{P} \in \phi(\Gamma)$ if and only if $\overline{x}$ is the square of a rational number.

Proof. a) $\phi(O) = \overline{O}$. Hence $\phi(\Gamma)$ is a subgroup of $\overline{\Gamma}$.

b) Let P=(x, y) $\in \Gamma$ s.t. $\phi(P) = \overline{O}$. Then $x \neq 0$ since that would mean that y=0 $\implies P = T$ and $\phi(T) = \overline{O}$. So $y^2/x^2 = 0$ means y=0.So,

$$0 = x^3 + ax^2 + bx = x(x^2 + ax + b) \tag{90}$$

This equation has non-zero rational root iff $a^2 - 4b$ is perfect square.

c)Let $\overline{P}$ be such point, then $\overline{x} = y^2/x^2$ is the square of a rational number. Conversely let $\overline{x} = w^2$ for some $w \in \mathbb{Q}$. We want to find a rational point on C that maps to $(\overline{x}, \overline{y})$. The homomorphism ϕ has two elements in its kernel, O and T . Thus if $(\overline{x}, \overline{y}) \in \phi(\Gamma)$, there will be two points in Γ that map to it.Let

$$x_1 = \frac{1}{2}(w^2 - a + \frac{\overline{y}}{w}),\ y_1 = x_1 w \tag{91}$$

$$x_2 = \frac{1}{2}(w^2 - a - \frac{\overline{y}}{w}),\ y_2 = -x_2 w \tag{92}$$

Verify that the points $P_i = (x_i, y_i)$ are on C and that $\phi(P_i) = (\overline{x}, \overline{y})$ for i = 1, 2. Since P_1 and P_2 are clearly rational points, this will prove that $(\overline{x}, \overline{y}) \in \phi(\Gamma)$.(It is very helpful in verification to note that $x_1 x_2 = b$) □

Proposition 4.12. *Let C, $\overline{C}, \phi, \psi, \Gamma$ and $\overline{\Gamma}$ be as before. Let $\mathbb{Q}^*$ be multiplicative group of $\mathbb{Q}$ and*

$$\mathbb{Q}^{*2} = \{u^2 : u \in \mathbb{Q}^*\} \tag{93}$$

Define a map α from $\overline{\Gamma}$ to $\mathbb{Q}^*/\mathbb{Q}^{*2}$) as follows:

$$\alpha(P) = \begin{cases} 1(mod\mathbb{Q}^{*2}) \ if\ P = O \\ b(mod\mathbb{Q}^{*2}) \ if\ P = T \\ x(mod\mathbb{Q}^{*2}) \ if\ P = (x, y) \ where\ x \neq 0 \end{cases} \tag{94}$$

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

$$\frac{\Gamma}{\psi(\overline{\Gamma})} \to \frac{\mathbb{Q}^*}{\mathbb{Q}^{*2}} \tag{95}$$

(c) Let $p_1, p_2, ...p_t$ be the distinct primes dividing b. Then $\alpha(\Gamma)$ is contained in the subgroup of $\mathbb{Q}^*/\mathbb{Q}^{*2}$ consisting of the elements

$$\{\pm p_1^{e_1} p_2^{e_2} ......p_t^{e_t} : e_i = 0 \ or \ 1\} \tag{96}$$

(d) The index $(\Gamma : \psi(\overline{\Gamma}))$ is at most 2^{t+1}.

Proof. a)Observe that α sends inverses to inverses, because

$$\alpha(-P) = \alpha(x, -y) = \frac{1}{x}.x^2 \equiv \frac{1}{x} = \alpha(P)^{-1}(mod\mathbb{Q}^{*2}) \tag{97}$$

Hence in order to prove that α is a homomorphism, it is enough to show that whenever $P_1 + P_2 + P_3 = O$, then $\alpha(P_1)\alpha(P_2)\alpha(P_3) \equiv 1(mod\mathbb{Q}^{*2})$. When P_1, P_2, P_3 are distinct then they are collinear. Let y = $\lambda x + \nu$ be line passing through them. Then $x_1x_2x_3 = \nu^2$(substitute the equation of line in C).Hence,

$$\alpha(P_1)\alpha(P_2)\alpha(P_3) = x_1x_2x_3 = \nu^2 \equiv 1(mod\mathbb{Q}^{*2}) \tag{98}$$

When P_1, P_2, P_3 are not distinct then also the result is valid(this can be checked).
b) There is a symmetric form of Lemma 4.11 for ψ. By that form, we get that $\psi(\overline{\Gamma})$ is the set of points (x, y) $\in \Gamma$ s.t. x $\in \mathbb{Q}^{*2}$, together with O, and also T if b is a perfect square. By this information and definition of α, it is clear that kernel of α is precisely $\psi(\overline{\Gamma})$.

c)Let P=(x, y)=($\frac{m}{e^2}, \frac{n}{e^3}$) $\in \Gamma$. Substitute this into C,

$$n^2 = m^3 + am^2e^2 + bme^4 = m(m^2 + ame^2 + be^4) \tag{99}$$

Let d = $gcd(m, m2 + ame^2 + be^4) \implies d|m, b.$
Since $n^2 = m(m^2 + ame^2 + be^4)$, means that every prime dividing m appears to an even power except possibly for primes dividing b. Hence, $\alpha(P)$ lies in indicated set. Above is not valid if x = 0 i.e. m = 0. But then by definition $\alpha(T) = b(mod\mathbb{Q}^{*2})$ means that the conclusion is still valid because, up to squares, b can be written in the indicated form. d) From b) and c), this is immediate. □

Lemma 4.13. *Let A and B be abelian groups, and let $\phi : A \to B$ and $\psi : B \to A$ are homomorphisms satisfying*

$$\psi \circ \phi(a) = 2a \ \forall \ a \in A \ and \ \phi \circ \psi(b) = 2b \ \forall \ b \in B. \tag{100}$$

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 indices satisfy

$$(A : 2A) \leq (A : \psi(B))(B : \phi(A)). \tag{101}$$

Proof. Since ψ(B) has finite index in A, let $a_1, ..., a_n$ be the representatives of the finitely many cosets. Similarly, since ϕ(A) has finite index in B, let $b_1, ..., b_m$ be representatives of the finitely many cosets.Consider the set

$$\{a_i + \psi(b_j) : 1 \leq i \leq n, 1 \leq j \leq m\} \tag{102}$$

It is easy to prove that above set contains a complete set of representatives for the cosets of 2A in A. □

Lemma 4.14. *Let $C : y^2 = x^3 + ax^2 + b$ be a elliptic curve. Then the index $C(\mathbb{Q}) : 2C(\mathbb{Q})$ is finite.*

Proof. Let A=$\Gamma = C(\mathbb{Q})$ and B= $\overline{\Gamma} = \overline{C}(\mathbb{Q})$ then by Prop 4.10(c) and Prop 4.11(d) conditions of lemma 4.13 are satisfied.(to get finite index of ϕ(A) in B, find the corresponding symmetric form for ϕ i.e. define the map α in Prop 4.12 from $\overline{\Gamma}$ to $\mathbb{Q}^*/\mathbb{Q}^{*2}$). Hence by lemma 4.13 the result follows. □

Theorem 4.15. ***(Mordell's Theorem)****(for curves with a rational point of order two) Let C be a non-singular cubic curve given by an equation $C : y^2 = x^3+ax^2+bx$, where a and b are integers. Then the group of rational points $C(\mathbb{Q})$ is a finitely generated abelian group.*

Proof. Using lemmas 4.4, 4.5, 4.9, 4.13 and theorem 4.1, the result follows. □

References

[1] Rational Points on Elliptic Curves- Joseph H. Silverman and John T. Tate

[2] Abstract Algebra- David S. Dummit and Richard M. Foote