RATIONAL POINTS OF FINITE ORDER ON ELLIPTIC CURVES

MINH-ANH NGUYEN-DANG

Abstract. This paper discusses Rational Points of Finite Order on Elliptic Curves. Assuming minimal knowledge, this paper goes over the basics of Projective Geometry, then discusses special points on Elliptic Curves, and concludes with the Nagell-Lutz Theorem.

Contents

1. Projective Geometry

1.1. **Projective Plane.** To get an intuitive understanding of the projective plane, we will discuss both algebraic and geometric definitions of the plane. We will first start with the algebraic definition.

1.1.1. *Algebraic Definition.*

Definition 1.1. Let $\mathbb{F}$ be a field. The *projective plane* $\mathbb{P}^2$ is the set of equivalence classes $[a, b, c]$ with a, b, c not all zero and $a, b, c \in \mathbb{F}$. Define the equivalence relation $\sim$ of $\mathbb{P}^2$ as

$$[a, b, c] \sim [a', b', c'] \text{ if } a = ta', b = tb', c = tc' \text{ for some nonzero } t.$$

More generally,

Date: DEADLINES: Draft AUGUST 14 and Final version AUGUST 28, 2024.

Definition 1.2. Let $n \in \mathbb{N}$. The *projective* n-space is the set of equivalance classes of homogeneous $n+1$ tuples:

$$\mathbb{P}^n = \frac{\{[a_0, a_1, ..., a_n] \mid a_0, a_1, ..., a_n \text{ not all zero}\}}{\sim}$$

where $a_0, a_1, ..., a_n \in \mathbb{F}$.

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

$$\alpha X + \beta Y + \gamma Z = 0.$$

1.1.2. *Geometric Definition.* We have the affine plane $\mathbb{A}^2$ as

$$\mathbb{A}^2 = \{(x, y) \mid x, y \in \mathbb{F}\}.$$

Definition 1.4. Thus we define the projective plane to be

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

Definition 1.5. We say a point A is a *point at infinity* when it is in $\mathbb{P}^2$ but not in $\mathbb{A}^2$–these points are associated with directions in $\mathbb{A}^2$.

So, a line in $\mathbb{P}^2$ then consists of a line in $\mathbb{A}^2$ together with the point at infinity specified by the line's direction. In the affine plane, two lines are parallel if and only if they have the same direction. Therefore, in $\mathbb{P}^2$, two "parallel lines" meet at the point of infinity corresponding to their common direction. Thus there are no parallel lines at all in $\mathbb{P}^2$.

Now we will inspect the set of directions in $\mathbb{A}^2$. Since every line in $\mathbb{A}^2$ is parallel to a unique line through the origin, these lines through the origin are given by the equation

$$Ay = Bx$$

with A and B not both zero. Note that, a pair of points (A', B') can produce the same line as (A, B) if $A' = tA$ and $B' = tB$ for some t. Therefore, the set of directions in $\mathbb{A}^2$ is naturally described by the set of points $[A, B]$ in $\mathbb{P}^1$.

Thus we have

$$\mathbb{P}^2 = \mathbb{A}^2 \cup \mathbb{P}^1.$$

1.1.3. *Relating the two definitions together.* We associate a point $(x, y) \in \mathbb{A}^2$ to the point $[x, y, 1] \in \mathbb{P}^2$. Similarly, a point $[a, b, c] \in \mathbb{P}^2$ with $c \neq 0$ corresponds to $(\frac{a}{c}, \frac{b}{c}) \in \mathbb{A}^2$. The points where $c = 0$ belong to $\mathbb{P}^1$.

Now, we will check that the lines match up. A line $L \in \mathbb{P}^2$, according to definition (1.3) is the set of solutions $[a, b, c]$ to the equation

$$\alpha X + \beta Y + \gamma Z = 0.$$

If α and β are not both zero, then any point $[a, b, c] \in L$ with $c \neq 0$ is sent to the point

$$\left(\frac{a}{c}, \frac{b}{c}\right) \text{ on } \alpha x + \beta y + \gamma = 0 \text{ in } \mathbb{A}^2.$$

The point $[-\beta, \alpha, 0] \in L$ is sent to the point in $\mathbb{P}^1$, which corresponds to the direction of the line $-\beta y = \alpha x$, which is the line parallel to L.

Now, if α and β are both zero, then $L : Z = 0$, which is the line that contains all points at infinity in $\mathbb{P}^2$.

1.2. **Curves in the Projective Plane.**

Definition 1.6. A polynomial $F(X, Y, Z)$ is called a *homogeneous polynomial* of degree d if it satisfies

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

The above identity also means that F is a linear combination of monomials $X^i Y^j Z^k$ with $i + j + k = d$.

Definition 1.7. A *projective curve* C in $\mathbb{P}^2$ to be the set of solutions to a polynomial equation

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

where F is a non-constant homogeneous polynomial. The degree of the curve is the degree of the polynomial F.

1.2.1. *Dehomogenization.* If we define a new, non-homogeneous polynomial $f(x, y)$ as

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

then the curve $f(x, y) = 0$ is called the affine part of C.

For a curve $C : F(X, Y, Z) = 0$, we can write C as the union of its affine part $C_0 : f(x, y) = 0$ and points pertaining to C_0's direction. The process of replacing the homogeneous polynomial with its affine part is called dehomogenization.

1.2.2. *Homogenization.* Given a polynomial $f(x, y)$ and its corresponding curve C_0, we want to find the projective curve C whose affine part is C_0. This is equivalent to finding the polynomial $F(X, Y, Z)$ such that $F(X, Y, Z) = f(x, y)$.

We have $f(x, y) = \sum a_{ij} x^i y^j$. The degree of f, say d, is the largest value of $i + j$ for which the coefficient a_{ij} is not zero.

Then, the *homogenization* of a polynomial $f(x, y)$ of degree d is defined to be

$$F(X, Y, Z) = \sum_{i,j} a_{ij} X^i Y^j Z^{d-i-j}.$$

We see that F is homogeneous with degree d, $F(x, y, 1) = f(x, y)$, and our choice of d ensures that $F(x, y, 0) \neq Z = 0$, so it does not contain the line at infinity.

Through dehomogenization and homogenization, we have established a one-to-one correspondence between a polynomial's affine part and projective part.

1.2.3. *Tangent line to a curve.* If $C : f(x, y) = 0$ is an affine curve, then implicit differentiation gives the relation

$$\frac{\partial f}{\partial x} + \frac{\partial f}{\partial y} \frac{dy}{dx} = 0.$$

The tangent line to C at the point (r, s) is given by

$$\frac{\partial f}{\partial x}(r,s)(x-r) + \frac{\partial f}{\partial y}(r,s)(y-s) = 0.$$

Definition 1.8. A singular point P of a curve $C : f(x, y) = 0$ if

$$\frac{\partial f}{\partial x}(P) = \frac{\partial f}{\partial y}(P) = 0.$$

Definition 1.9. We say the curve C is smooth (or non-singular) if every point on the curve is smooth.

If C is a curve given by an equation $C : f(x, y) = 0$, then we factor f into a product of irreducible polynomials

$$f(x,y) = p_1(x,y)p_2(x,y)....p_n(x,y).$$

The irreducible components of curve C are the curves

$$p_1(x,y) = 0, p_2(x,y) = 0, ..., p_n(x,y) = 0.$$

If C_1 and C_2 are two curves, we say that C_1 and C_2 have no common components if their irreducible components are distinct.

2. Points on Elliptic Curves

2.1. **Point at Infinity on Elliptic Curves.** We are considering $\mathbb{F} = \mathbb{R}$.

Given a Weierstrass equation

$$y^2 = x^3 + ax^2 + bx + c, \tag{2.1}$$

by letting $x = \frac{X}{Z}$ and $y = \frac{Y}{Z}$, we get a homogeneous equation:

$$Y^2Z = X^3 + aX^2Z + bXZ^2 + cZ^3. \tag{2.2}$$

We now want to find the point at infinity $\mathcal{O}$ where the cubic (2.2) intersects the line at infinity $Z = 0$. When $Z = 0$, we have $X^3 = 0$, thus $X = 0$, and so we have found the point at infinity $\mathcal{O} : [0, 1, 0]$. We can easily check that $\mathcal{O}$ is non-singular.

Now, we see that the direction of the line $X = 0$ is orthogonal to the $x-$axis, so all vertical lines (i.e. lines where x is constant) will meet at $\mathcal{O}$ per section 1.

So all lines intersect our cubic at three points: the infinity line meets the cubic three times at $\mathcal{O}$, vertical lines meet the cubic two times in the $xy-$plane and at $\mathcal{O}$, and any other line meets the cubic three times in the $xy-$plane. Note that, a line tangent to a point P on the cubic will meet the cubic three times, all at P.

2.2. **Group of Points on Elliptic Curves.** We will prove that the points on the cubic (2.1) form a group with $\mathcal{O}$ as the identity element.

Let P, Q be points on the cubic. Draw a line through P and Q, and denote the third intersection with the curve as $P * Q$. Let $+$ be an operation defined as follows:

$$P + Q = O * (P * Q).$$

In words, $P + Q$ is the third intersection point of the cubic and the line through $\mathcal{O}$ and $P * Q$.

By our definition, we see that + is a binary operation. We will now verify the identity element $\mathcal{O}$, the existence of inverses, and the associativity of the operation.

(1) $\mathcal{O}$ is the identity element:

Proof. Let P be a point on the cubic, and l be the line joining P and $\mathcal{O}$. Let $P * O$ be the third point of intersection between l and the cubic. We see that $O * (P * O) = P$, and so $P + O = O * (P * O) = P$. □

(2) The existence of inverses:

Proof. Let P be a point on the cubic. Since a cubic in the Weierstrass form is symmetric about the $x-$axis, let P' be the reflected point about the $x-$axis.

We will show that $P + P' = \mathcal{O}$. Indeed, the line l connecting P and P' is vertical, therefore it goes through $\mathcal{O}$ and so $\mathcal{O}$ is the third intersection point. Connecting $\mathcal{O}$ and $\mathcal{O}$ gives the line of infinity, and the third intersection is again $\mathcal{O}$. Therefore, $P + P' = \mathcal{O} * (P * P') = \mathcal{O} * \mathcal{O} = \mathcal{O}$. □

(3) Associativity of the operation:

Let P, Q, R be points on the cubic. We want to prove that

$$(P + Q) + R = P + (Q + R).$$

Due to the way the operation + is defined, it makes sense for us to prove

$$(P + Q) * R = P * (Q + R). \tag{2.3}$$

On the left hand side, we have lines

- $l1$: connecting P and Q, and so contains $P * Q$
- $l2$: connecting $P * Q$ and $\mathcal{O}$, thus contains $P + Q$
- $l3$: connecting $P + Q$ and R, thus contains $(P + Q) * R$.

On the right hand side, we have lines

- l4: connecting Q and R, and so contains $Q * R$
- l5: connecting $Q * R$ and $\mathcal{O}$, thus contains $Q + R$
- l6: connecting $Q + R$ and P, thus contains $P * (Q + R)$.

Now, to prove (2.3), we want to prove the intersection K of $l3$ and $l6$ lies on the cubic. We observe that there are nine points in consideration

$$\mathcal{O}, P, Q, R, P * Q, P + Q, Q * R, Q + R, K.$$

The first eight have already belong to the curve, and now we want the ninth to also be on the curve. It is natural for us to use the Cayley-Bacharach Theorem.

Theorem 2.4 (Cayley-Bacharach Theorem)**.** *Let C_1 and C_2 be projective curves with no common components with respective degrees d_1 and d_2. Let D be a curve in $\mathbb{P}^2$ with degree $d_1 + d_2 - 3$. If D passes through all but one of the points in $C_1 \cap C_2$, then D must also pass through the remaining point.*

We now want to construct C_1 and C_2 going through all nine points. Through multiplying three linear equations we get a cubic equation–so by multiplying the equations of $l1, l3, l5$ together and $l2, l4, l6$ together, we get two cubics and two corresponding curves C_1 and C_2 that go through all nine points. Since P, Q, R are all distinct points, the two curves C_1 and C_2 have no common components. Now, the original curve C goes through the first eight, and so by the Cayley-Bacharach Theorem, C also goes through the ninth.

Therefore, the operation + satisfies associativity.

2.3. **Points of Order Two and Three.**

Theorem 2.5. *Let C be a non-singular cubic curve*

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

a. *A point $P : (x, y) \neq \mathcal{O}$ on C has order two if and only if $y = 0$.*

Proof. $P \neq \mathcal{O}$ is a point on C with order two if and only if $2P = \mathcal{O}$. This means $P = -P$, so $(x, y) = (x, -y)$, and therefore $y = 0$. □

b. *The curve C has only four points of order dividing two. These four points form a group that is a product of two cyclic groups of order two.*

Proof. From part a, we conclude that points of order two are roots of $f(x)$.

Since $f(x)$ has three distinct roots due to the non-singularity of C, we have three points P_1, P_2, P_3 corresponding to the three roots, and so they are points of order two.

Also, note that since $\mathcal{O}$ is the identity element of C, $\mathcal{O}$ also has order dividing two.

Therefore, the curve C has four points of order dividing two: $\mathcal{O}, P_1, P_2, P_3$. □

c. *A point $P : (x, y) \neq \mathcal{O}$ on C has order three if and only if x is a root of the polynomial*

$$\psi_3(x) = 3x^4 + 4ax^3 + 6bx^2 + 12cx + 4ac - b^2.$$

Proof. A point $P : (x, y) \neq \mathcal{O}$ has order three if and only if $2P = -P$, which means $x(2P) = x(-P)$.

Using the duplication formula, we have the $x-$coordinate of a point $2P$ equals:

$$\frac{x^4 - 2bx^2 - 8cx + b^2 - 4ac}{4x^3 + 4ax^2 + 4bx + 4c}.$$

and so since $x(2P) = x(-P)$, we have

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

Multiplying each side with $4x^3 + 4ax^2 + 4bx + 4c$, we have

$$x^4 - 2bx^2 - 8cx + b^2 - 4ac = 4x^4 + 4ax^3 + 4bx^2 + 4cx$$

and so

$$3x^4 + 4ax^3 + 6bx^2 + 12cx + 4ac - b^2 = 0,$$

which means x is the root of the polynomial

$$\psi_3(x) = 3x^4 + 4ax^3 + 6bx^2 + 12cx + 4ac - b^2.$$

□

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.

Proof. We have $x(2P)$ equals

$$\frac{f'(x)^2}{4f(x)} - a - 2x,$$

and so since $x(2P) = x(P)$, we can substitute into $\psi_3(x)$ and attain

$$\psi_3(x) = 2f(x)f''(x) - f'(x)^2.$$

Now, we will prove that $\psi_3(x)$ has four distinct roots by showing that $\psi_3'(x)$ and $\psi_3(x)$ have no common roots.

We have

$$\psi_3'(x) = 2f(x)f'''(x) = 12f(x),$$

and so if $\psi_3(x)$ and $\psi_3'(x)$ were to have a common root, it would be a common root of $f(x)$ and $f'(x)$, whicih is a contradiction to the fact that C is non-singular.

Therefore, $\psi_3(x)$ have four distinct roots. Let x_1, x_2, x_3, x_4 be the four distinct roots of $\psi_3(x)$ and $y_i = \sqrt{f(x_i)}$ for $i \in \{1, 2, 3, 4\}$. From part c, we know that the set

$$\{(x_1, \pm y_1), (x_2, \pm y_2), (x_3, \pm y_3), (x_4, \pm y_4)\}$$

is the complete set of points of order three on C. Also note that there are no y_i that can equal to 0, since that would mean the point would have order two.

The only other point with order dividing three is $\mathcal{O}$.

Finally, note that the group

$$\{(x_1, \pm y_1), (x_2, \pm y_2), (x_3, \pm y_3), (x_4, \pm y_4), \mathcal{O}\}$$

is the product of two cyclic groups of order three. □

3. The Nagell-Lutz Theorem

Theorem 3.1. *(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 the polynomial

$$D = -4a^3 + a^2b^2 + 18abc - 4b^3 - 27c^2.$$

Let $P = (x, y)$ be a rational point of finite order. Then x and y are integers, and either $y = 0$ or y divides D.

We will tackle this theorem in several steps:

(1) We will show that if $P = (x, y)$ is a rational point of finite order, then x and y are integers.
(2) If P has order two, then $y(P) = 0$, or we will show that $y(P)$ divides D.

3.0.1. *Rational Points of Finite Order are Integers.* Let $P : (x, y)$ be a rational point with finite order on the curve C for $x = \frac{a}{b}$ and $y = \frac{c}{d}$. We will show that x and y are integers by showing that for every prime number p, $p \nmid b$ and $p \nmid d$.

Now, for every prime number p and a non-zero rational number x, we can express

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

for m, n are integers prime to p and the fraction $\frac{m}{n}$ is at its lowest terms. We will now introduce a definition:

Definition 3.2. The order of a rational number is the exponent v. This order depends on the choice of p.

We will prove that rational points of finite order are integers through the following proposition:

Proposition 3.3. *Let p be a prime, and let R be the ring of rational numbers with denominator prime to p. Let $C(p^v)$ be the set of rational points (x, y) on our curve for which x has denominator divisible by p^{2v} together with the point $\mathcal{O}$.*

a. $C(p)$ contains all rational points (x, y) for which the denominator of either x or y is divisible by p.
b. For every $v \geq 1$, the set $C(p^v)$ is a subgroup of the group of rational points $C(\mathbb{Q})$.

We will first prove part a. We can easily see the inclusion

$$C(\mathbb{Q}) \supset C(p) \supset C(p^2) \supset ....$$

and now we will prove that if the denominator of y is divisible by p, then the denominator of x is divisible by p^2.

Let (x, y) be a rational point on the curve with the denominator of y divisible by p. Thus we can express

$$x = \frac{m}{np^i} \text{ and } y = \frac{u}{wp^k}$$

where $k > 0$ and m, n, u, w are prime to p.

Plugging this point into our cubic equation, we get

$$\frac{u^2}{w^2p^{2k}} = \frac{m^3 + am^2np^i + bmn^2p^{2i} + cn^3p^{3i}}{n^3p^{3i}}. \tag{3.4}$$

Since $p \nmid u^2$ and $p \nmid w^2$,

$$\text{ord}\left(\frac{u^2}{w^2p^{2k}}\right) = -2k < 0. \tag{3.5}$$

Assume for the sake of contradiction that $i \leq 0$, and so our right hand side of (3.4) will have a non-negative order, which is a contradiction to (3.5). Therefore, $i > 0$. Note that $p \nmid m^3$, so

$$\text{ord}\left(\frac{m^3 + am^2np^i + bmn^2p^{2i} + cn^3p^{3i}}{n^3p^{3i}}\right) = -3i. \tag{3.6}$$

Combining (3.5) and (3.6), we get that $2k = 3i$, so i is divisible by 2. Hence $i \geq 2$.

Turning to part b, since we want to prove that $C(p^v)$ is closed under the operation $+$, we now want the point at infinity $\mathcal{O}$ at a finite place so we can perform the operation more efficiently.

We hope to move the point of infinity $\mathcal{O}$ to the point $(0, 0)$ through a change of coordinates. Let

$$t = \frac{x}{y} \text{ and } s = \frac{1}{y}. \tag{3.7}$$

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

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

in the (t, s)-plane. We can check that the zero element $\mathcal{O}$ is at $(0, 0)$ in the $(t, s)-$plane. Note that the $(t, s)-$plane excludes points where $y = 0$, i.e., points of order two.

Going from the $(t, s)-$plane back to the $(x, y)-$plane is also easy, as $y = \frac{1}{s}$ and $x = \frac{t}{s}$. Therefore, there is a one-to-one correspondence between the (t, s)-plane and the (x, y)-plane, except for points of order two.

Now we check if a line in the $(x, y)-$plane corresponds to a line in the $(t, s)-$plane. Let $y = \lambda x + v$ be a line in the $(x, y)-$plane. Divding the line by vy, we get

$$\frac{1}{v} = \frac{\lambda x}{vy} + \frac{1}{y}, \text{ so } s = -\frac{\lambda}{v}t + \frac{1}{v}.$$

Having checked both points and lines in the $(t, s)-$plane, we can "add" points in the $(t, s)-$plane under the same operation $+$ in $(x, y)-$plane.

Now, let $v \in \mathbb{N}$. Let (x, y) be a rational point in the $(x, y)-$plane lying in $C(p^v)$, so we can write

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

Then

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

Until now we only have definitions that concern with p in the denominator, and here we see p in the numerator. We also want to work with another structure bigger than groups for the sake of convenience. Therefore it is natural to consider the ring R_p which contains all rational numbers with no p in the denominator–one can easily check that these rational numbers indeed form a ring. The units in R are just the rational numbers with both the numerator and the denominator prime to p.

Thus our point (t, s) is in $C(p^v)$ if and only if $t \in p^v R$ and $s \in p^{3v} R$. This means p^v divides the numerator of t and p^{3v} divides the numerator of s. Moving to this ring will enable us, as we will see later, to prove closeness of the operation more seamlessly.

Let $P_1 = (t_1, s_1)$ and $P_2 = (t_2, s_2)$ be distinct points in $C(p^v)$. We will now, step by step, find the explicit formula for $P_1 + P_2$.

The first step is to find the line that goes through P_1 and P_2. There are two cases, the first one being $t_1 = t_2$ and the second one being $t_1 \neq t_2$.

If $t_1 = t_2$, then the vertical line $t = t_1$ meets C_1 at the third point $P_3 = (t_1, s_3)$, where P_3 may equal P_1 or P_2. So $P_1 + P_2$ will be $(-t_1, -s_3)$, so the $t(P_1 + P_2) \in p^v R$, and we attain $P_1 + P_2 \in C(p^v)$.

Now, if $t_1 \neq t_2$, we let $s = \alpha t + \beta$ be the line through P_1 and P_2, where

$$\alpha = \frac{s_2 - s_1}{t_2 - t_1}. \tag{3.8}$$

On the other hand, notice that (t_1, s_1), (t_2, s_2) satisfy the equation

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

and so

$$s_2 - s_1 = ({t_2}^3 - {t_1}^3) + a({t_2}^2 s_2 - {t_1}^2 s_1) + b(t_3 {s_2}^2 - t_1 {s_1}^2) + c({s_2}^3 - {s_1}^3).$$

Subtituting the above into (3.8) we get

$$\alpha = \frac{{t_2}^2 + t_1 t_2 + {t_1}^2 + a(t_2 + t_1)s_2 + b{s_2}^2}{1 - a{t_1}^2 - bt_1(s_2 + s_1) - c({s_2}^2 + s_1 s_2 + {s_1}^2)}. \tag{3.9}$$

Note that if $P_1 = P_2$, then the slope of a tangent line to C at P_1 is

$$\alpha = \frac{ds}{dt}(P_1) = \frac{3{t_1}^2 + 2at_1 s_1 + b{s_1}^2}{1 - a{t_1}^2 - 2bt_1 s_1 - 3c{s_1}^2},$$

which is the same as subtituting $t_1 = t_2$ and $s_1 = s_2$ into (3.9).

Now that we have roughly determined the line intersecting P_1 and P_2, we will now want to compute $P_1 + P_2$. Let $P_3 = (t_3, s_3)$ be the third point of intersection of the line $s = \alpha t + \beta$ with the curve. Subtituting $s = \alpha t + \beta$ into (3.7), we get

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

and so

$$0 = (1 + a\alpha + b\alpha^2 + c\alpha^3)t^3 + (\alpha\beta + 2b\alpha\beta + 3c\alpha^3 + \beta)t^2 + ... \tag{3.10}$$

Note that the equation on the right hand side of (3.10) has roots t_1, t_2, t_3, which means it equals to

$$C \cdot (t - t_1)(t - t_2)(t - t_3)$$

for C as some constant. Multiplying out, the equation above equals

$$C \cdot (t^3 - (t_1 + t_2 + t_3)t^2 + ...).$$

Comparing coefficients of t^3 and t^2, we get

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

If $t_1 + t_2 + t_3 \in p^{3v}R$, then we immediately get $t_3 \in p^{3v}R$ since $t_1, t_2 \in p^{3v}R$. So now we will look at α and β. Revisiting (3.9):

$$\alpha = \frac{{t_2}^2 + t_1t_2 + {t_1}^2 + a(t_2 + t_1)s_2 + b{s_2}^2}{1 - a{t_1}^2 - bt_1(s_2 + s_1) - c({s_2}^2 + s_1s_2 + {s_1}^2)}.$$

we can conclude that the numerator of α is in $p^{2v}R$ because each of t_1, s_1, t_2, s_2 is in p^vR. Similarly,

$$-a{t_1}^3 - bt_1(s_2 + s_1) - c({s_2}^2 + s_1s_2 + {s_1}^2) \in p^{2v}R$$

and so the denominator of α is a unit in R. Hence, $\alpha \in p^{2v}R$. Next, we have β is obtained by $s_1 - \alpha t_1$. Note that since $s_1 \in p^{3v}R$, $\alpha \in p^{2v}R$ and $t_1 \in p^vR$, it follows that $\beta \in p^{3v}R$.

Therefore, by a similar argument, we obtain

$$t_1 + t_2 + t_3 \in p^{3v}R \tag{3.11}$$

and immediately we get $t_3 \in p^{3v}R$. The function and the operation + also gives us the point $P_1 + P_2 = (-t_3, -s_3)$, therefore $P_1 + P_2 \in p^{3v}R$.

Since being in $p^{3v}R$ also means being in $C(p^v)$, we have successfully proven that $C(p^v)$ are subgroups of $C(\mathbb{Q})$ for all $v \in \mathbb{N}$.

Now we will use the above proposition to prove that if $P = (x, y) \in C(\mathbb{Q})$ are points of rational orders, then x and y are integers.

First, (3.11) is equivalent to

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

thus we get

$$t(P_1 + P_2) \equiv t(P_1) + t(P_2) \pmod{p^{3v}R}.$$

Back to the proof, let $P \in C(\mathbb{Q})$ be a point of order m with $m \geq 2$. Let p be a prime. Assume for the sake of contradiction that $P \in C(p)$. Let $v = \frac{1}{2}\text{ord}(x)$, therefore $P \in C(p^v)$ and $P \notin C(p^{v+1})$.

If $p \nmid m$, then using the congruence

$$t(P_1 + P_2) \equiv t(P_1) + t(P_2) \pmod{p^{3v}R}$$

we get

$$t(mP) \equiv mt(P) \pmod{p^{3v}R.}$$

Since $mP = \mathcal{O}$, we have $t(mP) = t(\mathcal{O}) = 0$. Also since m is prime to p, we attain

$$0 \equiv t(P) \pmod{p^{3v}R}.$$

Therefore, $P \in C(p^{3v})$, contradicting the assumption that $P \notin C(p^{v+1})$.

If $p \mid m$, we can write $m = pn$. Consider the point $P' = (x', y')$ such that $nP' = P$. Since P has order n, it follows that P' has order p. As $P \in C(p)$ and $C(p)$ is a subgroup of $C(\mathbb{Q})$, we have $P' \in C(p)$. Let $v = \frac{-1}{2}\text{ord}(x')$, we get $P' \in C(p^v)$ while $P' \in C(p^{v+1})$. By a similar argument as the above scenario, we have

$$0 = t(\mathcal{O}) = t(pP') \equiv pt(P') \pmod{p^{3v})R}.$$

Therefore

$$t(P') \equiv 0 \pmod{p^{3v-1})R}.$$

Since $3v - 1 \geq v + 1$, this contradicts our assumption.

We have proven that if $P = (x, y)$ is a point of finite order, then $P \notin C(p)$ for all primes p. It follows that the denominators of x and y are divisible by no primes, hence x and y are both integers.

This concludes the first part of the theorem.

3.0.2. *Y-Coordinates of Rational Points of Finite Order divides D.*. We will now prove the second part of the Theorem.

Let $P = (x, y)$ be a rational point of finite order, so by the first part of our problem, P has integer coordinates. By section 2, we know that if P has order two, then $y = 0$.

Now, assume that $y \neq 0$. We will show that $y \mid D$.

Recall the discriminant D of our Weirstrass equation is

$$D = -4a^3c + a^2b^2 + 18abc - 4b^3 - 27c^2.$$

Also recall our polynomial is

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

hence its derivative is

$$f'(x) = 3x^2 + 2ax + b.$$

Let

$$r(x) = (18b - 6a^2)x - (4a^3 - 15ab + 27c)$$

and

$$s(x) = (2a^2 - 6b)x^2 + (2a^3 - 7ab + 9c)x + (a^2b + 3ac - 4b^2).$$

Notice that $r(x)$ and $s(x)$ are polynomials with integer coefficients. Furthermore, one can easily check that

$$D = r(x)f(x) + s(x)f'(x) \tag{3.12}$$

Using the duplication formula, we have

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

Since x, X and a are all integers and λ is a rational number, it follows that λ is also an integer. Now, since $2y$ and $f'(x)$ are both integers, we have $2y \mid f'(x)$, which leads to $y \mid f'(x)$. Now, since $y^2 = f(x)$ (our Weierstrass equation), we get $y \mid f(x)$.

Since the polynomials $r(x)$ and $s(x)$ both have integer coordinates, when plugging the integer x into those polynomials, they will take on integer values. Combining with (3.12) and the fact that $y \mid f(x)$ and $y \mid f'(x)$, we get $y \mid D$. This completes the proof.

4. Acknowledgements

I would like to thank my mentor, Pranjal Warade, for supporting me throughout this year's REU. I would also like to thank Professor May for organizing such a wonderful research experience for undergraduates. Lastly, I would like to thank my friends who have made this summer of math memorable.

5. References

Silverman, Joseph H., and John Torrence Tate. Rational Points on Elliptic Curves. Springer International Publishing, 2015.

Dummit, David Steven, and Richard M. Foote. Abstract Algebra. John Wiley & Sons, 2016.