Rational Points on Elliptic Curve

Full name: LiuBaihan

ID: Liu190OSRP21

August 2021/08/08

*This dissertation is my own work and includes nothing which is the outcome of work done in collaboration expect as specified in the text. It is not substantially the same as any work that has already been submitted before for any degree or other qualification except as specified in the text. It does not exceed the agreed word limit.

Abstract

This dissertation explores some properties of rational points on elliptic curve, where we mainly focus on studying non-singular cubic curve in Weierstrass normal form. We define the group law of elliptic curve in a geometric way and derive duplication formula based on the group law. Nagell-Lutz Theorem tells us an interesting property of points of finite order, which says that rational points of finite order have integer coordinates. The theorem also provides a way to find possible points of finite order. We prove Nagell-Lutz Theorem by contradiction and provides some inspiring examples. In addition, we also point out the Mazur's Theorem, which tells us the group structure of rational points of finite order. We then move to study rational points over finite field. We find the Reduction Modulo p theorem which gives an alternative way to find the group consisting of points of finite order. Finally, we study integer points on elliptic curve. Siegel's Theorem tells us that non-singular cubic curve with integer coefficients has only finitely many points with integer coordinates. Siegel's Theorem can be proved by Diophantine Approximation Theorem.

Contents

1 Introduction

We will follow the exposition given in "Rational Points on Elliptic Curves"(Second Edition) by Tate and Silverman [**1**], but will explore the topics with different focus.

2 Geometry and Arithmetic

We are interested in finding the rational solutions of the Diophantine equations in two variables.

2.1 Rational solutions to linear polynomials and quadratic polynomials

The set of real solutions to a polynomial equation $f(x, y) = 0$ forms an algebraic curve in xy-plane. The graphs of linear polynomials are straight lines. The graphs of quadratic polynomials are conic sections. The followings are some definitions.

Definition 2.1 *The set of rational point in the plane is:*

$$\mathbb{Q}^2 = \{(x, y), x, y \in \mathbb{Q}\}.$$

The set of rational line in the plane is:

$$L = \{ax + by + c = 0, a, b, c \in \mathbb{Q} \text{ and } a, b, c \text{ are simplified}\},$$

The set of rational conics in the plane is:

$$C = \{ax^2 + bxy + cy^2 + dx + ey + f = 0, a, b, c, d, e, f \in \mathbb{Q} \text{ and they are simplified}\}.$$

The rational solutions to linear polynomials and quadratic polynomials with rational coefficients are well-known. The reasons are as follows.

The intersection between any two non-parallel rational lines is rational. Moreover, for any rational line, x is rational if and only if y is rational. Therefore, x can be any rational number and thus there are infinitely many solutions.

In general, the intersection between a rational conic and a rational line is not rational, because the roots of the quadratic equation for the x-coordinates of the intersection points might be conjugate quadratic irrationals. However, since the sum of roots for a quadratic polynomial is rational, if one of the root is rational, then we can guarantee that another root must as well be rational. As a result, if we find a rational point $\mathcal{O}$ on a conic, we can choose a rational line and project the conic onto the line from $\mathcal{O}$. The intersection points on the conic and on the line are all rationals. In this way, we get a one-to-one correspondence between the points on the conic and the points on the line. (We ignore the case of projecting $\mathcal{O}$ itself onto the line, it needs some knowledge of projective geometry.)

Example 2.1 *To find all rational points on the circle*

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

we can project from the point $(1, 1)$ *onto the rational line* $y = -x$. *The intersection point is* $(t, -t)$. *The figure is shown below.*

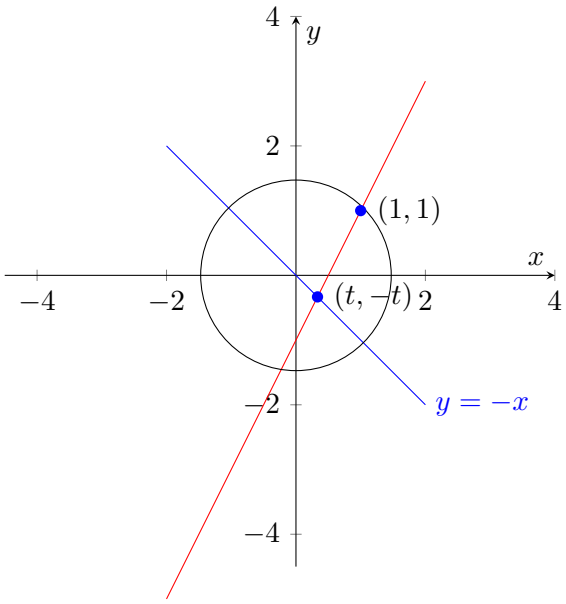

Figure 1:Finding rational points on a circle

The equation connecting $(1,1)$ *to* $(t,-t)$ *is*

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

Combining equation (1) and equation (2) and use the equation of sum of roots for quadratic polynomial, we find

$$x = \frac{5t-1}{1-t}$$

and

$$y = \frac{7t^2+2t-1}{(1-t)^2}.$$

To represent t *in* x, y*, we find*

$$t = \frac{y-x}{y+x-2}.$$

x, y *are rational if and only if* t *is rational. This gives a one-to-one correspondence between points on the circle* $x^2+y^2=2$ *and points on the line* $y=-x$*.*

2.2 Non-singular cubic curve in Weierstrass normal form

A cubic with Weierstrass form look like $y^2 = x^3 + ax^2 + bx + c$. Using projective geometry, we can show that any cubic is birationally equivalent to a cubic of this form. Thus, we can restricted our focus on studying rational points on cubic curves in Weierstrass normal form.

We write the cubic equation as

$$F(x,y) = y^2 - f(x) = 0$$

The partial derivatives are

$$\frac{\partial F}{\partial x} = -f'(x), \qquad \frac{\partial F}{\partial y} = 2y.$$

A cubic curve is singular provided that there is at least a point on the curve at which both partial derivatives simultaneously vanish. A cubic curve is non-singular if the polynomial $f(x)$ has distinct roots. In later case, the partial derivative will not vanishes.

Proposition 2.1 *For a cubic curve $y^2 = f(x) = x^3 + ax^2 + bx + c$, the determinant $D = -4a^3c + a^2b^2 + 18abc - 4b^3 - 27c^2 \neq 0$ if and only if the roots of $f(x)$ are distinct. In other words, $D \neq 0$ if and only if $f(x)$ is non-singular.*

Proof 2.1 *Let $\alpha_1, \alpha_2, \alpha_3$ be the three roots of $f(x)$.*

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

$$D = (\alpha_1 - \alpha_2)^2(\alpha_2 - \alpha_3)^2(\alpha_1 - \alpha_3)^2.$$

Therefore, $D \neq 0$ if and only if the roots of $f(x)$ are distinct.

Singular cubic curves are easy to be treated as a conics. Geometrically, these graphs have cusps, self-interactions, or isolated points. As a result, by using the same approaches as conics, we can also easily find all the rational points on singular cubic curves. Therefore, we will mainly focus on finding rational solutions on non-singular cubic curves.

2.3 The origin of the name "elliptic curve"

A cubic curve is called an elliptic curve. This is because cubic curves have something to do with the arc length of ellipses.

Theorem 2.1 *For an elliptic C*

$$\frac{x^2}{\alpha^2} + \frac{y^2}{\beta^2} = 1, \quad 0 < \beta \leq \alpha$$

The arc length of the ellipse is

$$\int_0^1 \frac{1 - k^2t^2}{u}\, dt$$

where

$$u^2 = (1 - t^2)(1 - k^2t^2)$$

which is an elliptic curve, and

$$k^2 = 1 - \frac{\beta^2}{\alpha^2}.$$

Proof 2.2 *We give a parametrization of the elliptic curve.*

$$x = \alpha\cos(\theta), y = \beta\sin(\theta)$$

where $\theta \in [0, 2\pi]$. *The differential arc length is*

$$ds = \sqrt{(\frac{dx}{d\theta})^2 + (\frac{dy}{d\theta})^2}d\theta$$

Using the formula $\sin(\theta)^2 + \cos(\theta)^2 = 1$ *and formula* $\cos(\theta) = \sin(\frac{\pi}{2} - \theta)$,

We find that the arc length is

$$4\alpha\int_0^{\frac{\pi}{2}} \sqrt{1 - k^2\sin(\theta)^2}\, d\theta.$$

We change variable θ *to* t *by* $t = \sin(\theta)$. *We get*

$$4\alpha\int_0^{\frac{\pi}{2}} \sqrt{1 - k^2\sin(\theta)^2}\, d\theta = 4\alpha\int_0^1 \frac{1 - k^2t^2}{\sqrt{(1 - t^2)(1 - k^2t^2)}}\, dt$$

$$= \int_0^1 \frac{1 - k^2t^2}{u}\, dt$$

If C *is not a circle, then the equation*

$$u^2 = (1 - t^2)(1 - k^2t^2)$$

defines an elliptic curve. The proof is omitted here. Therefore, to determine the arc length of the elliptic curve, we just need to evaluate the integral

$$= \int_0^1 \frac{1 - k^2t^2}{u}\, dt$$

on the elliptic curve

$$u^2 = (1 - t^2)(1 - k^2t^2).$$

2.4 Interpretation of the Group Law

There is no specific quick way to determine whether a rational cubic has a rational point. Thus, we assume that our cubic curves have rational points.

We give a geometry interpretation of the group law and we denote the group law by $+$. The identity point $\mathcal{O}$ is a non-singular point at infinity. There is only one point of infinity by point of projective geometry. The following figure shows the rule of addition +.

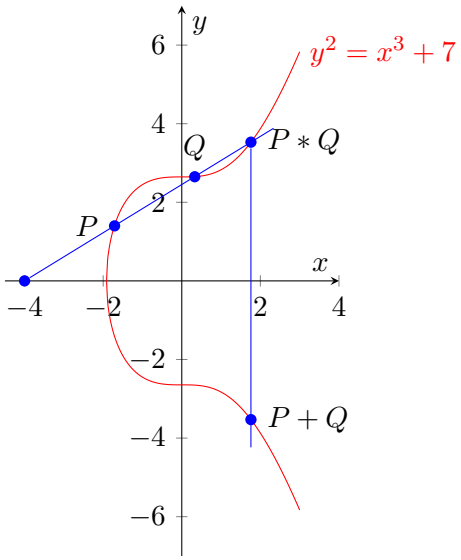

Figure 2: Group law on elliptic curve

To add P and Q, we draw a line through P and Q and take the third intersection point as $P * Q$. We reflect it about x-axis and gain $P + Q$. To find the addition of a point P to itself, we draw a tangent line to the cubic at P to get $P * P$. The tangent line can be seemed as meeting the cubic twice at P. The inverse of P is a reflection point about x-axis. The set of rational points on an elliptic curve is

$$\Gamma = \{(x, y) : y^2 = x^3 + ax^2 + bx + c, x, y \in \mathbb{Q}\} \cup \{\mathcal{O}\},$$

which forms a commutative group with group law $+$. Verification steps and their corresponding figures are as follows.

- Closure: If P and $Q \in \Gamma$, then $P + Q \in \Gamma$.
- Associative law:$(P + Q) + R = P + (Q + R)$.
- The identity element:$P + \mathcal{O} = \mathcal{O} + P = P$.
- The inverse: $P + (-P) = (-P) + P = \mathcal{O}$.
- Commutative: $P + Q = Q + P$.

This steps can be proved in a geometric way or in an algebraic way.

2.5 Duplication formula

For a rational point P in the elliptic curve

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

we aim to derive an equation to find x and y coordinates of $2P$. The tangent line at point $P = (x_0, y_0)$ is $y = \lambda x + \nu$. The slope λ of the tangent line is the same as the slope of elliptic curve at point P, which is $\frac{f'(x_0)}{2y_0}$. In addition, since P is on both the tangent line and the elliptic curve, we can set an equation:

$$y^2 = (\lambda x + \nu)^2 = x^3 + ax^2 + bx + c.$$

We can obtain a cubic equation in x,

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

The equation has a double root at x_0 and a root at $x(2P)$. Thus,

$$x^3 + (a - \lambda^2)x^2 + (b - 2\lambda\nu)x + (c - \nu^2) = (x - x_0)^2(x - x(2P)).$$

Equating the coefficients, we find that

$$x(2P) = \lambda^2 - a - 2x_0$$

and

$$y(2P) = -(\lambda x(2P) + \nu).$$

Therefore, we can derive the duplication formula,which is

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

for rational point $P = (x, y)$. We can also calculate the y-coordinate for $2P$ by

$$y(2P) = -(\lambda x(2P) + \nu).$$

$f(x)$ has distinct root since we assume the cubic curve is non-singular. Therefore, $f'(r) \neq 0$ for any root r of $f(x)$, which means that in this case, the numerator and the denominator of $x(2P)$ have no common (complex) roots.

2.6 Find nP

1. Method I: Let $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$, then $P_1 * P_2 = (x_3, y_3)$ and $P_1 + P_2 = (x_3, -y_3)$. The line joining P_1 and P_2 has slope $\frac{y_2 - y_1}{x_2 - x_1}$. Using a similar procedure as section 2.5, we find that

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

   We write $nP = (x_n, y_n)$ and use $nP = (n-1)P + P$. The explicit formula for the group law is

   $$x_n = (\frac{y_{n-1} - y_1}{x_{n-1} - x_1})^2 - a - x_{n-1} - x_1.$$

2. Method II: In this method, we use duplication formula to find nP. We can use duplication

formula to solve $n = 2^k, k \geq 1$. We can express any integer n in base two. In other words, we can express any integer n as a sum of powers of two. For example, $n = 21 = 2^4 + 2^2 + 1$. Thus, we can find nP for any integer n. In most cases, Method II is more efficient than Method I.

3 Points of Finite Order

3.1 Points of order two and three

Definition 3.1 *An element P of any group have order m if $mP = \mathcal{O}$, but $m'P \neq \mathcal{O}, 1 \leq m' \leq m$. P has finite order if m exists.*

3.1.1 Points of order two

For a non-singular cubic curve C, a point $P = (x, y)$ has order two if and only if $y = 0$. This is because $P = (x, y) = (x, -y) = -P$. Thus, the curve has exactly four points of order two dividing two, denote the set of these points as $\{\mathcal{O}, P_1, P_2, P_3\}$. $P_1 + P_2 + P_3 = 0$ because they are colinear. All of the points satisfying $2P = \mathcal{O}$ forms a subgroup in any abelian group.

The fact is that any group of order 4 is either cyclic or isomorphic to the "Klein-Four Group". Since every element in this group is of order one or two, the group is a "Klein-Four Group", which can be represented as a product of two cyclic group of order 2.

3.1.2 Points of order three

Proposition 3.1 *A point $P = (x, y) \neq \mathcal{O}$ on C has order three if and only if x is a root of the polynomial*

$$\psi_3(x) = 3x^4 + 4ax^3 + 6bx^2 + 12cx + 4ac - b^2 = 0.$$

Proof 3.1 *A point has order three if and only if $x(2P) = x(P)$. Using the duplication formula in section 1.5, we can formulate an equation $3x^4 + 4ax^3 + 6bx^2 + 12cx + 4ac - b^2 = 0$.*

Proposition 3.2 *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 3.2 *Since*

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

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

Claim: $\psi_3(x)$ has four distinct (complex) roots.

Proof of claim: To verify the statement in the claim, it is equivalent to prove that $\psi_3(x)$ and $\psi_3(x)^2$ have no common roots. We suppose for contradiction that they have common roots. As a result, there exists a common root of $2f(x)f''(x) - f'(x)^2$ and $12f(x)$. Thus, this means that there is a common root of $f(x)$ and $f'(x)$, which contradicts to our assumption. Therefore, $\psi_3(x)$ has four distinct (complex) roots, denoted them as $\beta_1, \beta_2, \beta_3, \beta_4$. The set of points of order three will be

$$\{(\beta_1, \pm\delta_1), (\beta_2, \pm\delta_2), (\beta_3, \pm\delta_3), (\beta_4, \pm\delta_4)\} \cup \{\mathcal{O}\}.$$

Since the $(\beta_i, \pm\delta_i)$ has order three, $\delta_i \neq 0$. The curve C has nine points of order divding three and they form a group that is a product of two cyclic groups of order three.

A geometric interpretation of points of order three:

$$3P = \mathcal{O} \Leftrightarrow 2P = -P \Leftrightarrow P * P = P.$$

Thus, $3P = \mathcal{O}$ means that the third intersection point on the tangent line through P is just P.

3.2 Nagell-Lutz Theorem

Theorem 3.1 (Nagell-Lutz Theorem) *For a cubic curve $y^2 = f(x) = x^3 + ax^2 + bx + c$,*

1. *If (x, y) is a rational point of finite order, then its coordinates are integers.*
2. *For a point of this type, either $y = 0$ or $y^2|D$, where $D = -4a^3c + a^2b^2 + 18abc - 4b^3 - 27c^2$ is the discriminant of the polynomial $f(x)$.*

Remark 1 *The theorem implies that a cubic curve has only finite rational points of finite order.*

We can use this theorem to find all possible points of finite order. Since the converse of this theorem is not true, we should check whether the points we find have finite order or not.

Proof 3.3 *1. We prove this by showing that when x and y are written in lowest terms, there is no prime p that divide the denominator of x and the denominator of y.*

Definition 3.2 (p-adic valuation) *The p-adic valuation of a non-zero integer n is the largest power of prime that divides n, denoted as $\nu_p(n)$. It is the exact power appearing in the prime factorization of n.*

p-adic valuation can be generalized to rational numbers. For a rational number $\frac{a}{b}$, $\frac{a}{b} = p^k\frac{m}{n}$, where $m, n \in \mathbb{Z}$ and p does not divide m, n. Then, the p-adic valuation of $\frac{a}{b}$, $\nu_p(\frac{a}{b})$, is equal to k.

Proposition 3.3 *If $\nu_p(a) = k_1$ and $\nu_p(b) = k_2$, then $\nu_p(\frac{a}{b}) = \nu_p(p^{k_1-k_2}\frac{m}{n}) = \nu_p(a) - \nu_p(b)$.*

Definition 3.3 *We define the order of a rational number to be the exponent ν.*

$$ord(\frac{m}{n}p^\nu) = \nu,$$

where $m, n \in \mathbb{Z}$ are prime to p and $\frac{m}{n}$ is in lowest terms.

Remark 2 *The order of a rational number is just the the p-adic valuation of a rational number. In other words, $ord(\frac{m}{n}p^\nu) = \nu = \nu_p(\frac{m}{n}p^\nu)$.*

Definition 3.4 *Let $C(p^\nu)$ be the set of rational points (x, y) on our curve for which x has denominator divisible by $p^{2\nu}$, including the point $\mathcal{O}$.*

$$C(p^\nu) = \{(x, y) \in C(\mathbb{Q}) : ord(x) \leq -2\nu \; and \; ord(y) \leq -3\nu\} \cup \{\mathcal{O}\}$$

We have an sequence of inclusions from the definition of $C(p^\nu)$.

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

Definition 3.5 *Let R_p be the ring of rational numbers with denominator prime to p.*

$$R_p = \{\frac{a}{b} \in \mathbb{Q} : p \nmid b\}$$

If $p \nmid b$, then $\frac{a}{b} = p^k \frac{m}{n}$, where $k \geq 0$. We let $ord(0) = \infty$ by convention.

Hence,

$$R_p = \{\frac{a}{b} \in \mathbb{Q} : \nu_p(\frac{a}{b}) \geq 0\}.$$

Proposition 3.4 *(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 the group of rational points $C(\mathbb{Q})$.

(c) The map

$$\frac{C(p^\nu)}{C(p^{3\nu})} \longrightarrow \frac{p^\nu R_p}{p^{3\nu} R_p},$$

$$P = (x, y) \mapsto t(P) = \frac{x}{y},$$

is a one-to-one homomorphism. (We send $\mathcal{O} \longrightarrow 0$ by convention.)

Proof 3.4 *(a) For a rational point (x, y) on the cubic curve $y^2 = x^3 + ax^2 + bx + c$, we assume that p divides the denominator of x. We write*

$$x = \frac{m}{np^\mu} \quad and \quad y = \frac{u}{wp^\sigma},$$

where $\mu > 0$. In addition, we assume p does not divide m, n, u or w. We plug this point into the equation $y^2 = x^3 + ax^2 + bx + c$ and compare the orders between the two sides. We have $2\sigma = 3\mu$.

Therefore, $\mu = 2\nu$ and $\sigma = 3\nu$ for some integer $\nu > 0$. We can carry out a similar

procedure for the case when p divides the denominator of y. Thus, if p divides the denominator of x or the denominator of y, then p divides both of them. In this case, the exact power for x and y are $p^{2\nu}$ and $p^{3\nu}$, respectively.

Therefore, if p divide the denominator of x or y, then there is at least a p^2 in x and a p^3 in y. We can conclude that $C(p)$ consists of all rational points (x, y) for which the denominator of either x or y is divisible by p.

(b) The point of infinity $\mathcal{O}$ is in $C(p^\nu)$, so $C(p^\nu)$ is clearly nonempty. We are going to change coordinates from (x, y) to (t, s). Let

$$t = \frac{x}{y} \quad and \quad s = \frac{1}{y}.$$

Intuitively, the mapping sends the point at infinity in (x, y)-plane to $(0, 0)$ in (t, s)-plane while moves the point of order two in (x, y)-plane to the point of infinity in (t, s)-plane. For all other points, they are mapped bijectively between (x, y)-coordinates and (t, s)-coordinates. We can show that

$$(t, s) \in C(p^\nu) \iff t \in p^\nu R_p \text{ and } s \in p^{3\nu} R_p.$$

For a line in (x, y)-plane $y = \lambda x + \nu$, it corresponds to a line in (t, s)-plane $s = -\frac{\lambda}{\nu} t + \frac{1}{\nu}$.

Thus, we can add points in the same way in (t, s)-plane as in (x, y)-plane. Let $P_1 = (t_1, s_1)$ and $P_2 = (t_2, s_2)$ on $C(p_\nu)$. If $t_1 = t_2$, then the t-coordinate of $P_1 + P_2$ is $-t_3$ by the group law of the elliptic curve.

Thus, we assume $t_1 \neq t_2$. The line connecting the two points $s = \alpha t + \beta$ intersects with the cubic at the third point $P_3 = (t_3, s_3)$. $P_1 + P_2 = (-t_3, -s_3)$ since the identity point in (t, s)-plane is $(0, 0)$. If $P_1 = P_2$, then $\alpha = \frac{ds}{dt}(P_1)$. If P_1 and P_2 are distinct, then $\alpha = \frac{t_1 - t_2}{s_1 - s_2}$. In both cases, we obtain β by $\beta = s_1 - \alpha t_1$. Combining equations $s = \alpha t + \beta$ and $y^2 = x^3 + ax^2 + bx + c$ and comparing coefficients, we

have

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

We can find that

$$s_1 \in p^{3\nu}R_p, \alpha \in p^{2\nu}R_p, t_1 \in p^{\nu}R_p, \text{ and } \beta \in p^{3\nu}R_p.$$

Thus,

$$t_1 + t_2 + t_3 \in p^{3\nu}R_p.$$

$$t_1, t_2 \in p_3{}^{\nu}R_p \Longrightarrow -t_3 \in p^{3\nu}R_p.$$

If $t \in p^{\nu}$*, then* $-t \in p^{\nu}$*. Thus, if* $P = (t, s) \in C(p^{\nu})$*, then* $-P = (-t, s) \in C(p^{\nu})$*.*

In summary, we have

i. $C(p^{\nu}) \subset C(\mathbb{Q})$.

ii. $C(p^{\nu}) \neq \emptyset$.

iii. $P_1, P_2 \in C(p^{\nu}) \Longrightarrow P_1 + P_2 \in C(p^{\nu})$.

iv. $P \in C(p^{\nu}) \Longrightarrow -P \in C(p^{\nu})$.

We conclude that $C(p^{\nu})$ *is a subgroup of* $C(\mathbb{Q})$.

(c) From (b), we have

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

The first addition is the addition defined in the cubic curve, while the second addition is the normal addition of rational numbers. Thus, there is a well-defined homomorphism

$$\phi : C(p^{\nu}) \longrightarrow \frac{p^{\nu}R_p}{p^{3\nu}R_p}.$$

Since

$$ker(\phi) = C(p^{3\nu}) \text{ and } im(\phi) = \frac{p^{\nu}R_p}{p^{3\nu}R_p}.$$

By First Isomorphism Theorem, this is a one-to-one homomorphism (isomorphism)

$$\frac{C(p^\nu)}{C(p^{3\nu})} \longrightarrow \frac{p^\nu R_p}{p^{3\nu} R_p},$$

$$P = (x, y) \mapsto t(P) = \frac{x}{y}.$$

Corollary 3.1 *(a) For every prime p, the only point of finite order in the group $C(p)$ is the identity point. In other words, if $nP = \mathcal{O}$ and $P \in C(p)$, then $P = \mathcal{O}$.*

(b) Let $P = (x, y) \in C(\mathbb{Q})$ be a rational point of finite order, then x and y are integers.

Proof 3.5 *(a) Let $nP = \mathcal{O}$ and $P \in C(p)$. Suppose for contradiction that $P \notin C(p)$. Let ν be the largest one among all $\nu > 0$ satisfying $P \in C(p^\nu)$, which means $P \in C(p^\nu)$ and $P \notin C(p^{\nu+1})$. Specifically, $\nu = -\frac{1}{2}ord(x)$.*

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

Repeating this formula, we get

$$0 = t(\mathcal{O}) = t(nP) \equiv nt(P) \pmod{p^{3\nu} R_p}.$$

i. When n is prime to p,

$$0 \equiv t(P) \pmod{p^{3\nu} R_p}.$$

Thus,

$$P \in C(p^{3\nu}) \subset C(p^{\nu+1}),$$

which contradicts to the fact that $P \notin C(p^{\nu+1})$.

Therefore, $nP = \mathcal{O}$ and $P \in C(p)$.

ii. When $n = mp$, let $P' = (x', y') = mP$. P' has order p, so it has order dividing

n. *Thus,* $P' \in C(p)$. *Let* $\nu = -\frac{1}{2}ord(x')$, *so* $P' \in C(p^\nu)$ *and* $P' \notin C(p^{\nu+1})$.

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

Thus,

$$P' \in C(p^{3\nu-1}) \subset C(p^{\nu+1}),$$

which contradicts to the fact that $P' \notin C(p^{\nu+1})$.

(b) *If* $P = (x, y)$ *is a point of finite order, which means that* $nP = \mathcal{O}$ *for some* n, *then we know from (a) that either* $P \neq \mathcal{O}$ *or* $P \notin C(p)$ *for all primes* p. *Thus,* $P = \mathcal{O}$ *or* $P = (x, y)$ *where* $x, y \in \mathbb{Z}$.

2. *If* P *has finite order,* $2P$ *will also have finite order. Thus, both* P *and* $2P$ *have integer coordinates. Let* $\phi(x) = 4f(x)x(2P)$. *There exist a degree-3 polynomial* $F(x)$ *and a degree-2 polynomial* $\Phi(x)$ *both with integer coefficients such that*

$$F(x)f(x) + \Phi(x)\phi(x) = D$$

$F(x)$ *and* $\Phi(x)$ *can be obtained by equating coefficients. If* $y = 0$, *then* $2P = \mathcal{O}$. *If* $y \neq 0$, $\phi(x) = 4f(x)x(2P)$. $2P$ *also has finite order, so we have* $x(2P) \in \mathbb{Z}$ *and hence* $f(x)|\phi(x)$. *Since* $y^2 = f(x)$, *we have* $y^2|f(x)$. *Thus,* $y^2 \mid F(x)f(x) + \Phi(x)\phi(x) = D$.

Corollary 3.2 *If there exist an integer* n *such that the coordinates of* nP *are not integers, then* P *has infinite order.*

Proof 3.6 *By Nagell-Lutz Theorem,* nP *does not have finite order because their coordinates are not integer. Therefore,* P *does not have finite order either.*

Corollary 3.3 *Let* C *be a non-singular elliptic curve* $y^2 = x^3 + ax^2 + bx + c$ *with integer coefficients and let* $P \in C(\mathbb{Q})$. *If* nP *has integer coordinates for some* $n \geq 1$, *then* P *has integer coordinates.*

Proof 3.7 *Since nP has integer coordinates, $nP \notin C(p)$ for all prime p. This is because by definition, $C(p)$ is the set of all points whose denominators is a multiple of p. We can deduce that $P \notin C(p)$, because otherwise, since $C(p)$ is a group, we will get a contradictory result, $nP \in C(p)$. Thus, P has integer coordinates.*

3.3 Find points of finite order by Nagell-Lutz Theorem

Example 3.1 *Let C be the cubic curve $y^2 = x^3 + px$, the discriminant of $f(x)$ is $D = -4p^3$. By Nagell-Lutz Theorem, all $(x, y) \in \Gamma$ which has finite order should satisfy $x, y \in \mathbb{Z}$ and $y = 0$ or $y^2|D$. Thus, the possible y are $0, \pm 1, \pm 2, \pm p, \pm 2p$.*

Lemma 3.1 *For a Diophantine equation with one variable,*

$$a_n x^n + a_{n-1} x^{n-1} + ... + a_1 x + a_0 = 0.$$

If $\frac{m}{n}$ is a rational solution written in lowest term, or $gcd(m, n) = 1$, then $m|a_0$ and $n|a_n$.

For a given y, we can use this lemma to find possible solutions of x.

Find possible points of finite order		
y	*Equation*	*Integer solutions*
0	$x^3 + px = 0$	$(0, 0)$
± 1	$x^3 + px - 1 = 0$	*no*
± 2	$x^3 + px - 4 = 0$	$(1, 2), (1, -2)$ *if* $p = 3$.
$\pm p$	$x^3 + px - p^2 = 0$	*no*
$\pm 2p$	$x^3 + px - 4p^2 = 0$	$(3, 6), (3, -6)$ *if* $p = 3$.

Table 1

From the above table, we see that there is no integer solution unless $p = 3$. When $p = 3$, the integer solutions are $(1, \pm 2)$ and $(3, \pm 6)$. Using duplication formula, we find that if we

double the integer points found above, the x-coordinates of them are $\frac{1}{4}$, which is not an integer. According to Corollary 4.2, these integer solution points do not have finite order.

All in all, the only rational points which have finite order are $(0,0)$ and $\mathcal{O}$.

Example 3.2 *We aim to find points of finite order and determine the structure of the group formed by the points of finite order.*

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

We should do some transformations about the equation. First, we complete the square.

$$y^2 - y + \frac{1}{4} = x^3 - x^2 + \frac{1}{4}$$

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

Replace y by $y - \frac{1}{2}$, we get

$$y^2 = x^3 - x^2 + \frac{1}{4}.$$

However, $\frac{1}{4}$ is not an integer. Therefore, we need to clear the denominator of this term.

We define a map which sends (x, y) to $(\frac{1}{4}, \frac{1}{8})$. Then we get

$$y^2 = x^3 - 4x^2 + 16.$$

$$a = -4, b = 0, c = 16$$

$$D = -2816 = 2^8 11$$

$$y = 0 \text{ or } y \mid 2^4.$$

Find possible points of finite order		
y	*Equation*	*Integer solutions*
0	$x^3-4x^2+16=0$	*no*
±1	$x^3-4x^2+15=0$	*no*
±2	$x^3-4x^2+12=0$	*no*
±4	$x^3-4x^2=0$	$(0,\pm4),(4,\pm4)$
±8	$x^3-4x^2-48=0$	*no*
±16	$x^3-4x^2-240=0$	*no*

Table 2

Let $P=(0,4)$, $Q=(0,-4)$.

$x(2P)=4,\ y(2P)=-4$, $x(4P)=0, y(4P)=-124$. *Then we have*

$x(2Q)=4,\ y(2Q)=4$, $x(4Q)=0, y(4Q)=124$.

Since the points $(0,\pm124)$ *are of infinite order, the points* $(0,\pm4)$ *and* $(4,\pm4)$ *are of infinite order. The point of finite order is* $\{O\}$. *The group is a trivial group.*

3.4 Mazur's Theorem

Lemma 3.2 *Let* Φ *be the set consisting of all points of finite order.*

$$\Phi=\{P=(x,y)\in C(\mathbb{Q}):P\ has\ finite\ order\}\cup\{\mathcal{O}\}.$$

The set Φ *is a subgroup of* $C(\mathbb{Q})$, *which we called torsion subgroup.*

Proof 3.8 *Let* P_1 *and* P_2 *be points of finite order. There must exist positive integers* m_1 *and* m_2 *such that* $m_1P_1=\mathcal{O}$ *and* $m_1P_1=\mathcal{O}$. *We have* $m_1m_2(P_1\pm P_2)=\mathcal{O}$, *so* $P_1\pm P_2$ *are of finite order. It is obvious that integer multiples of any point in* Φ *also lie in* Φ. *In conclusion,* Φ *is a subgroup of* $C(\mathbb{Q})$.

Theorem 3.2 (Mazur's Theorem) *Let* C *be a non-singular rational cubic curve, and suppose that* $C(\mathbb{Q})$ *contains a point of finite order* m. *Then the set of points of finite order in* $C(\mathbb{Q})$ *forms a subgroup that has one of the following forms:*

1. C_N *for* $N \in \{1, 2, ..., 10\}$ *or* C_{12}.

2. $C_2 \times C_{2N}$ *for* $N \in \{1, 2, 3, 4\}$.

4 Cubic Curves Over Finite Field

4.1 Rational points over finite fields

We will look at the rational points at the cubic curve

$$C : F(x, y) = 0$$

over $\mathbb{F}_p$, the field of integers modulo p, where p is a prime.

The set of rational points, including the point of infinity is

$$C(\mathbb{F}_p) = \{(x, y) : x, y \in \mathbb{F}_p \quad and \quad F(x, y) = 0\} \cup \{\mathcal{O}\}.$$

For a cubic curve $C : y^2 = x^3 + ax^2 + bx + c$, we desire to find the rational points over field $\mathbb{F}_p$. Since x and y are supposed to be in $\mathbb{F}_p$, we can take each of the p possibilities for x, put them into the polynomial $x^3 + ax^2 + bx + c$, and check if the result is a square in $\mathbb{F}_p$.

Since the possibilities of x and y are finite, the group $C(\mathbb{F}_p)$ is finitely generated. The question is that how to estimate the number of points in $C(\mathbb{F}_p)$.

Definition 4.1 *Let* $n, a \in \mathbb{N}$ *and* $gcd(a, n) = 1$. a *is quadratic residue modulo* n *if* $x^2 \equiv a \pmod{n}$. *Otherwise,* a *is a quadratic non-residue modulo* n.

Theorem 4.1 (Euler's Criterion) *Given an odd prime* p *and an integer* a *with the condition that* p *not divide* a, *the number* a *is a quadratic residue modulo* p *if and only if*

$$a^{\frac{p-1}{2}} \equiv 1 \pmod{p}.$$

the number a is a quadratic nonresidue modulo p if and only if

$$a^{\frac{p-1}{2}} \equiv -1 \pmod{p}.$$

Proposition 4.1 *If p is an odd prime, the congruence has either no solution or exactly two incongruent solutions $x^2 \equiv \pm x_0 \pmod{n}$. There are always $\frac{p-1}{2}$ quadratic residues and $\frac{p-1}{2}$ quadratic nonresidues.*

Therefore, given arbitrary x, y has 50% change to be a quadratic residues and 50% change to be a quadratic non-residues. Since there are p possible x in the finite field, there are approximately $2(\frac{p-1}{2}) + 1$ rational solutions including the point at infinity.

We can use Euler's Criterion to check whether a is a quadratic residue modulo p or not.

Lemma 4.1 *Let C be a non-singular irreducible curve defined over a finite field $\mathbb{F}_p$. An estimate of the number of in $C(\mathbb{F}_p)$ is equal to $p + 1 - \epsilon$, where ϵ is an error term.*

4.2 Reduction modulo p theorem

We define the map "reduction modulo p" by

$$\mathbb{Z} \longrightarrow \mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p,$$

$$z \mapsto \widetilde{z}$$

$$\widetilde{z} = z \mod p$$

$C : y^2 = x^3 + ax^2 + bx + c$ is an elliptic curve with integer coefficients. The reduced curve C modulo p is

$$\widetilde{C} : y^2 = x^3 + \widetilde{a}x^2 + \widetilde{b}x + \widetilde{c}.$$

If a point (x, y) on the curve has integer coordinates, then we can reduce that point modulo p. We get the equation

$$\widetilde{C} : \widetilde{y}^2 = \widetilde{x}^3 + \widetilde{a}\widetilde{x}^2 + \widetilde{b}\widetilde{x} + \widetilde{c}.$$

Theorem 4.2 *Let C be a non-singular cubic curve $y^2 = x^3 + a^2x^2 + bx + c$ with integer coefficients. Let Φ be the set consisting of all points of finite order.*

For any prime p, let $P \longrightarrow \widetilde{P}$ be the reduction modulo p map

$$\Phi \longrightarrow \widetilde{C}(\mathbb{F}_p),$$

$$\Phi \longrightarrow \widetilde{C}(\mathbb{F}_p) = \begin{cases} (\widetilde{x}, \widetilde{y}) \; if \; P = (x, y), \\ \widetilde{\mathcal{O}} \qquad if \; P = \mathcal{O}. \end{cases}$$

If p does not divide $2D$, then the reduction modulo p map is an isomorphism of Φ onto a subgroup of $\widetilde{\mathbb{F}_p}$.

Remark 3 *According to Nagell-Lutz Theorem, points of finite order have integer coordinates. Therefore, the reduction modulo p map is well-defined.*

Remark 4 *Reduction Modulo p Theorem sometimes reduces computation work. Compared to Nagell-Lutz Theorem, Reduction Modulo p Theorem is likely to be a more effective method to find the rational points of finite order.*

Proof 4.1 ***Lemma 4.2*** *The reduced curve $\widetilde{C} \pmod p$ is non-singular $\iff$ $p \geq 3$ and p does not divide D.*

Proof 4.2 *The reduction modulo p of the discriminant D is*

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

It is easy to see that the reduction modulo p map is a homomorphism. Thus, $\widetilde{D} = D \pmod p$. $\widetilde{D} = 0 \iff p \mid D$. This proves the above lemma.

The next step is to prove that the reduction modulo p map is a group homomorphism.

$$-\widetilde{P} = \widetilde{(x, -y)} = (\widetilde{x}, -\widetilde{y}) = -\widetilde{P}.$$

Let P_1, P_2 be two points $\in \Phi$, Let $P_3 = -(P_1 + P_2)$,

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

Thus,

$$\widetilde{P_1} + \widetilde{P_2} + \widetilde{P_3} = \mathcal{O} \iff \widetilde{P_1 + P_2} = \widetilde{P_1} + \widetilde{P_2}.$$

It suffices to show that if $P_1 + P_2 + P_3 = \mathcal{O}$, then $\widetilde{P_1} + \widetilde{P_2} + \widetilde{P_3} = \mathcal{O}$.

Suppose $P_1 + P_2 + P_3 = \mathcal{O}$. We let $y = \lambda x + \mu$ be the line through P_1, P_2 and P_3.

$$0 = x^3 + ax^2 + bx + c - (\lambda x + \mu)^2 = (x - x_1)(x - x_2)(x - x_3).$$

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

If we reduce modulo p, we obtain

$$x^3 + \widetilde{a}x^2 + \widetilde{b}x + \widetilde{c} - (\widetilde{\lambda}x + \widetilde{\nu}) = (x - \widetilde{x_1})(x - \widetilde{x_2})(x - \widetilde{x_3}).$$

We can also reduce $y_i = \lambda x_i + \nu$ to

$$\widetilde{y_i} = \widetilde{\lambda}\widetilde{x_i} + \widetilde{\nu} \text{ for } i = 1, 2, 3.$$

Thus, the line $\widetilde{y_i} = \widetilde{\lambda}\widetilde{x_i} + \widetilde{\nu}$ intersects $\widetilde{C}$ at $\widetilde{P_i}$ for $i = 1, 2, 3$. As a result, $\widetilde{P_1} + \widetilde{P_2} + \widetilde{P_3} = \widetilde{\mathcal{O}}$.

Therefore, the reduction modulo p map ϕ is a homomorphism. For every non-zero $(x, y) \in \Phi$, $(\widetilde{x}, \widetilde{y}) \in \widetilde{C}(\mathbb{F}_p)$ can not be $\widetilde{\mathcal{O}}$. Thus, the kernel of this map is $\{\mathcal{O}\}$ and hence the map is an isomorphism.

4.3 Examples of Reduction Modulo p Theorem

Example 4.1 *We aim to find the group Φ for the curve*

$$C : y^2 = x^3 + x + 1.$$

To find group consisting of all points of finite order, we find $D = 2^4 31$. *Thus,* 3 *and* 7 *do not divide* D.

$p = 3$		
x	$y^2 (\mod 3)$	*Integer solutions*
0	*1*	$(0,1)$, $(0,2)$
1	*3*	$(1,0)$
2	*2*	*no*

Table 3

$p = 7$		
x	$y^2 (\mod 7)$	*Integer solutions*
0	*1*	$(0,1)$, $(0,6)$
1	*3*	*no*
2	*4*	$(2,2)$, $(2,5)$
3	*3*	*no*
4	*6*	*no*
5	*5*	*no*
6	*6*	*no*

Table 4

Therefore,

$$\widetilde{C}(\mathbb{F}_3) = \{\mathcal{O}, (0,1), (0,2), (1,0)\}.$$

$$\widetilde{C}(\mathbb{F}_7) = \{\mathcal{O}, (0,1), (0,6), (2,2), (2,5)\}.$$

According to Reduction Modulo p Theorem, Φ *is a subgroup of* $\widetilde{C}(\mathbb{F}_3)$ *and* $\widetilde{C}(\mathbb{F}_7)$. *Then we have*

$$\#\Phi | gcd(\#\widetilde{C}(\mathbb{F}_3), \#\widetilde{C}(\mathbb{F}_7)) = 1$$

Thus, $\Phi = \{\mathcal{O}\}$, *which is the trivial group.*

Example 4.2 *c is sixth power free. We aim to find the group structure of the the set of points of finite order on the curve $C : y^2 = x^3 + c$*

$$\mathbb{F}_p{}^* = \mathbb{F}\backslash\{0\}.$$

$\mathbb{F}_p$ is a field. $\mathbb{F}_p{}^*$ is a multiplicative group with identity 1. It is a cyclic group of order $p-1$. If $p \equiv 2 \pmod 3$, we claim that the map $x \mapsto x^3$ is an isomorphism from $\mathbb{F}_p{}^*$ to itself.

Proof of the claim:

$$\phi : \mathbb{F}_p \longrightarrow \mathbb{F}_p{}^3$$

$$\phi(xy) = \phi(x)\phi(y) \quad \& \quad \phi(1).$$

Thus, ϕ is a homomorphism.

Since F_p* is a finite set,

ϕ is bijective $\iff$ ϕ is injective $\iff$ ϕ is surjective

Method I: we will show ϕ is injective.

$$ker(\phi) = \{x \in \mathbb{F}_p{}^* : x^3 \equiv 1 \pmod p\}$$

Then the order of x divides both 3 and $p-1$. Then the order of x divides both 3 and $p-1$.

Since $p \equiv 2 \pmod 3$ and $gcd(3, p-1) = 1$, then $ker(\phi) = \{1\}$ and thus ϕ is injective.

Method II: we will show ϕ is surjective.

Therefore, ϕ is a bijective homomorphism, which is an isomorphism. Since we also have $0 = 0^3$, every element in $\mathbb{F}_p$ has a unique cube root.

Combine everything, we have an isomorphism from x to x^3.

It is clear that $x \mapsto x + c$ and $x \mapsto x - c$ is a bijection.

Since there are $\frac{p-1}{2}$ quadratic residues in $\mathbb{F}_p$, there exists $2\frac{p-1}{2} + 1 = p + 1$ points on the cubic curve over the finite field. Thus, $\#C(\mathbb{F})_p = p + 1$.

Let p takes all values such that $p \equiv 2 \pmod 3$ and $p > 54c^2$. As a result, $p+1$ is even and $p + 1 \equiv 0 \pmod 3$. Then, $\#C(\mathbb{F}_p) = p + 1|6$. $\#\Phi|6$.

We now consider the possible abelian groups of order dividing 6.

Find Possible Size and Possible Group Structure of Φ			
Φ *contains a point of order two*	Φ *contains a point of order three*	$\#\Phi$	*The group that is isomorphic to* Φ
No	*No*	*1*	$\{\mathcal{O}\}$
Yes	*No*	*2*	$\mathbb{Z}/2\mathbb{Z}$
No	*Yes*	*3*	$\mathbb{Z}/3\mathbb{Z}$
Yes	*Yes*	*6*	$\mathbb{Z}/6\mathbb{Z}$

Table 5

From the table above, we can conclude that to find the group structure of Φ*, we only need to check whether or not* Φ *contains a point of order two or a point of order three.*

(x, y) *is a point of order two* $\iff y = 0 \iff x^3 + c = 0 \iff$ c *is a cube in* $\mathbb{Q}$*.*

(x, y) *is a point of both order two and order three* $\iff$ c *is both a square and a cube* $\iff$ $c = 1$.

(x, y) *is neither a point of both order two or a point of order three* $\iff$ Φ *is the trivial group.*

(x, y) *is a point of order three* $\iff$ x *is a root of* $\psi_3 = 3x(x^3 + 4c) \iff x = 0$ *or* $x = -4c$*.*

$x = 0 \iff y^2 = c \iff$ c *is a square in* $\mathbb{Q}$*.*

$x^3 = -4c \iff y^2 = x^3 + c = -3c \iff -4c$ *is a cube and* $-3c$ *is a square.*

Claim: $-4c$ *is a cube and* $-3c$ *is a square* $\iff c = -432$*.*

Proof of the Claim:

Method I:

$-3c$ *is a square* $\Longrightarrow c < 0$*. Besides,* c *is an non-zero integer. we can write* $c = -2^k 3^l {p_1}^{e_1} ... {p_r}^{e_r}$*, where* $k, l, e_1, ..., p_r$ *are distinct primes.*

Then, we have

$$-4c = -2^{k+2} 3^l {p_1}^{e_1} ... {p_r}^{e_r}$$

$$-3c = -2^k 3^{l+1} {p_1}^{e_1} ... {p_r}^{e_r}$$

$$-4c \text{ is a cube} \Longrightarrow \begin{cases} k+2 = 3z_1, \\ l = 3z_2, \\ e_i = 3m_i, i = 1, ..., r, \end{cases} \quad \text{for some } z_1 \in \mathbb{Z}^+,\ z_2, m_i \in \mathbb{Z}^+ \cup \{0\}.$$

$$-3c \text{ is a square} \Longrightarrow \begin{cases} k = 2z_3, \\ l+1 = 2z_4, \\ e_i = 2n_i, i = 1, ..., r, \end{cases} \quad \text{for some } z_4 \in \mathbb{Z}^+,\ z_3, n_i \in \mathbb{Z}^+ \cup \{0\}.$$

Combining them, we get $\begin{cases} \frac{z_1}{z_3+1} = \frac{2}{3}, \\ \frac{z_2+1}{z_4} = 2. \end{cases} \Longrightarrow \begin{cases} z_1 = 2, \\ z_2 = 1, \\ z_3 = 2, \\ z_4 = 2. \end{cases} \Longrightarrow \begin{cases} k = 4, \\ l = 3. \end{cases}$

and $e_i = 6m_in_i$.

Since c is sixth power free, $m_in_i = 0$ *for all i. Thus,* $c = -2^4 3^3 {p_1}^0 ... {p_r}^0 = -432$

Method II: Since $-4c$ *is a cube* $\Longrightarrow$*, we write* $-4c = a^3$*. According to the definition of p-adic valuation,* $V_2(c) + 2 = V_2(a^3)$*. Looking at the prime factorization of a, we see that* $V_2(a^3)$ *is a multiple of three.*

For $p > 2$*, we know* $V_p(c) = 3V_p(a)$*. Therefore,* $V_p(c)$ *is a multiple of three.*

Since $-3c$ *is a square, then* $-3c = b^2$*. According to the definition of p-adic valuation,* $V_3(c) + 1 = 2V_3(b)$*. Thus,* $V_3(c)$ *is odd. For* $p \neq 3$*,* $V_p(c)$ *is even. For* $p \neq 2, 3$*, we know that* $\nu_p(c)$ *is even and it is a multiple of three. Thus, it is a multiple of six.*

If $V_2(c) \geq 6$*, then* $2^6 \mid c$*, which contradicts to the condition that c is sixth power free. Assume* $\nu_2 \leq 5$*. Since* $V_2(c)$ *is even and* $V_2(c) + 2 = V_2(a^3)$*,* $V_2(c) = 4$*. Similarly, we show that* $V_3(c) = 3$*. Thus,*

$$c = -2^4 3^3 = -432.$$

In summary, we have

$$\Phi \cong \begin{cases} \mathbb{Z}/6\mathbb{Z} & if\ c = 1, \\ \mathbb{Z}/3\mathbb{Z} & if\ c \neq 1\ is\ a\ square,\ or\ if\ c = -432, \\ \mathbb{Z}/2\mathbb{Z} & if\ c \neq 1\ is\ a\ cube, \\ \{\mathcal{O}\} & otherwise. \end{cases}$$

Example 4.3 *For the elliptic curve $C : y^2 = x^3 + x$, we aim to show that $\#C(\mathbb{F}_p)$ is a multiple of four.*

Firstly, $\mathcal{O}$ is a point of finite order.

Claim: When $p \geq 3$, -1 is a square modulo $p \iff p \equiv 1 \pmod 4$.

Proof of Claim:

1. *If $p \equiv 3 \pmod 4$, suppose$x^2 \equiv -1 \pmod p$, then $x^4 \equiv 1 \pmod p$.*
   Since $p = 4k + 3$ for some $k \in \mathbb{Z}$,

$$x^{p-1} = x^2(x^4)^k \equiv -1 \pmod p,$$

   which contradicts Fermat's Little Theorem.

2. *If $p \equiv 1 \pmod 4$, then $p = 4k + 1$ for some $k \in \mathbb{Z}$.*

$$(-1)^{\frac{p-1}{2}} \equiv (-1)^{2k} \equiv 1 \pmod p.$$

   By Euler's Criterion, -1 is a square modulo p.

Thus, we prove the claim.

1. *If $p \equiv 1 \pmod 4$, -1 is a square modulo p. If $y = 0$,*

$$x^3 + x = x(x^2 + 1) \equiv 0 \pmod p.$$

$$x = 0\ or\ x^2 + 1 \equiv 0 \pmod p.$$

$x^2 + 1 \equiv 0 \pmod{p}$ *will have two solutions* λ *and* $-\lambda$*. Therefore,* $(0,0), (\lambda,0), (-\lambda,0)$ *are points of order two. Thus, we find four points of finite order,* $\mathcal{O}, (0,0), (\lambda,0)$ *and* $(-\lambda,0)$.

Next we focus on solutions where $x \neq 0$ *and* $y \neq 0$*. If* (x,y) *is a solution, then* $(x,-y)$ *is a solution. Since* $(-x)^3 + (-x) = -y^2 = (\lambda y)^2$*, then* $(-x,\lambda y), (-x,-\lambda y)$ *are also solutions. Hence the solutions come in fours. Thus,* $4 \mid |C(\mathbb{F}_p)|$.

2. *If* $p \equiv 3 \pmod{4}$*,* $x^2 + 1 \equiv 0 \pmod{p}$ *has no solution.* $\mathcal{O}$ *and* $(0,0)$ *are points of finite order.*

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

We introduce the Legendre symbol, $(\frac{a}{p}) = a^{(n-1)/2} \pmod{p}$*. By Euler's Criterion, we can prove a property of Legendre symbol.*

$$(\frac{ab}{p}) = (\frac{a}{p})(\frac{b}{p}).$$

In addition, $(\frac{-1}{p}) = -1$.

Thus,

$$(\frac{x^3+x}{p}) = -(\frac{(-x)^3+(-x)}{p}).$$

There are two cases.

If $x^3 + x$ *is a quadratic residue, then* $(-x)^3 + (-x)$ *is a non-quadratic residue. If* $x^3 + x$ *is a quadratic non-residue, then* $(-x)^3 + (-x)$ *is a quadratic residue.*

Using similar procedure as Example 4.2, we find that there is an isomorphism from x *to* $x^3 + x$*. Therefore, there are* $\frac{p-1}{2}$ x *give quadratic residue for* $x^3 + x$*. Each gives the cubic equation two solutions. There are* $\frac{p-1}{2}$ x *give quadratic non-residue for* $x^3 + x$*. Each gives no solution to the cubic equation. In total, there are* $2(\frac{p-1}{2}) + 1 - p + 1$ *solutions, which means that* $\#C(\mathbb{F}_p) = p + 1$.

Since $p \equiv 3 \pmod{4}$*, hence* $p + 1 \equiv 0 \pmod{4}$*. Then,* $4 \mid |C(\mathbb{F}_p)|$.

5 Integer Points on Cubic Curves

5.1 Siegel's Theorem

We aim to describe the integer points on the cubic curve.

The converse of Nagell- Lutz Theorem is not true. It means that points having integer coordinates may not have finite order.

Definition 5.1 (Siegel's Theorem) *Let C be a non-singular cubic curve given by an equation $F(x, y) = 0$ with integer coefficients. Then C has only finitely many points with integer coordinates.*

The proof of Siegel's Theorem can be transformed into the proof of Diaphantine Approximation Theorem.

5.2 Integer points on linear, quadratic, and singular cubic equation

For linear equations with integer coefficients, the equations have either no solution or infinitely many solutions.

Proposition 5.1 *For a linear polynomial $ax + by = c$, if $d = gcd(a, b)$ does not divide c, then the linear polynomial will fail to have integer coefficients. Otherwise, the linear polynomial will have infinitely many solutions. If there exist one integer solution (x_0, y_0) which is found by extended Euclidean Algorithm, then we can represent the whole solution set as $\{x_0 + k\frac{b}{gcd(a,b)}, y_0 - k\frac{a}{gcd(a,b)}, k \in \mathbb{Z}\}$.*

Proof 5.1 *1. We first prove that points in this set are solutions.*

$$a(x_0 + k\frac{b}{gcd(a,b)}) + b(y_0 - k\frac{a}{gcd(a,b)}) = ax_0 + by_0 = c.$$

2. Next we show that all solutions are in the set. Let (x_0, y_0) be any solution. We have

$$ax + by = c = ax_0 + by_0.$$

Then,

$$\frac{b}{d} \mid \frac{a}{d}(x - x_0)$$

Since $gcd(\frac{a}{d}, \frac{b}{d}) = 1$*,*

$$\frac{b}{d} \mid (x - x_0)$$

$$x = x_0 + k\frac{b}{d},\ k \in \mathbb{Z}$$

Similarly, we find

$$y = y_0 - k\frac{a}{d},\ k \in \mathbb{Z}$$

Quadratic equations with integer coefficients can also have infinitely many solutions. Consider the Pell's equation, $x^2 - dy^2 = 1$.

Theorem 5.1 *Suppose that* (x_1, y_1) *is the smallest positive solution to Pell's equation* $x^2 - dy^2 = 1$*, where* $d \in \mathbb{N}$ *and* d *is not a perfect square. Then the complete solution set to the equation is* $\{(x_n, y_n) : n \in \mathbb{N}\}$*, where* (x_n, y_n) *is given by* $x_n + y_n\sqrt{d} = (x_1 + y_1\sqrt{d})^n$*.*

Some singular curves have infinitely many integer points. For example, for any $t \in \mathbb{Z}$, $(t^2, t^3) \in C_1$ is an integer solution for the curve $C : y^2 = x^3$.

5.3 Integer points on cubic curves which have integer factorization

For cubic curvea which have integer factorization, there are finitely many solutions which we can find them in an elementary way. For example, Find integer solutions to $x^2y + xy^2 = 240$.

$$xy(x + y) = 240$$

$$A = x + y \text{ and } B = xy$$

$$x(A - x) = B$$

$$x^2 - Ax + B = 0$$

For each $AB = 240$, we check if $\frac{A \pm \sqrt{A^2 - 4B}}{2}$ is an integer. Among all possible cases of A and B, we find that there are two cases that make $A^2 - 4B$ a square: $A = 16$ and $B = 15$,

$A = 12$ and $B = 20$. Further calculation shows that these two cases indeed give us integer solutions. There are four integer points $(1, 15), (15, 1), (2, 10)$ and $(10, 2)$.

There are cubic curves that infinitely rational solutions.

$$C_d : y^2 = x^3 + d$$

$$C_d(\mathbb{Z}) = \{(x, y) : x, y \in \mathbb{Z} \text{ and } y^2 = x^3 + d\}$$

There exist d such that $y^2 = x^3 + d$ has infinitely many rational solutions. For example, when $d = 9$, $P = (3, 6)$ is on the curve $y^2 = x^3 + 9$. Then we have

$$x(2P) = \frac{x^4 - 72x}{4x^3 + 36} = -\frac{135}{144} \notin \mathbb{Z}.$$

Thus, $P = (3, 6)$ has infinite order and $y^2 = x^3 + 9$ has infinitely many rational solutions. Since there are infinitely many rational points on $y^2 = x^3 + 9$, we can certainly find N distinct points, say $P_1, ..., P_N$. If $P = (\frac{a}{b}, \frac{c}{d})$ is any rational point written in lowest terms with positive denominators.

$$\frac{a^2}{b^2} = \frac{c^3}{d^3} + 9$$

$$a^2d^3 = c^3b^2 + 9b^2d^3$$

Since $gcd(a, b) = 1$ and $gcd(c, d) = 1$, we get $b^2 \mid d^3$ and $d^3 \mid c^3b^2$ and thus $b^2 = d^3$. We can write $P_1, P_2, ..., P_N$ as

$$P_1 = (\frac{a_1}{b_1}, \frac{c_1}{{b_1}^{\frac{2}{3}}}), ..., P_N = (\frac{a_N}{b_N}, \frac{c_N}{{b_N}^{\frac{2}{3}}}).$$

We choose d to clear the denominators of P_i. Let $D = {b_1}^{\frac{5}{3}}{b_2}^{\frac{5}{3}}...{b_N}^{\frac{5}{3}}$. We take $d = 9D^6$. Then the points $P_i = (\frac{D^2a_i}{b_i}, \frac{D^3c_i}{{b_i}^{\frac{2}{3}}})$ for $i = 1, 2, ..., N$ have integer coordinates and are on the curve $y^2 = x^3 + 9D^6$.

6 Reference

[1] J.H. Silverman and J.T. Tate, Rational Points on Elliptic Curves, Springer (1992).