From String Theory to Elliptic Curves over Finite Field, $\mathbb{F}_p$

A Senior Project submitted to
The Division of Science, Mathematics, and Computing
of
Bard College

by
Linh Thi Dieu Pham

Annandale-on-Hudson, New York
May, 2014

Abstract

Superstring Theory is a study using supersymmetric strings to give an explanation for fundamental elements in the nature. One of its main focuses is an algebraic geometric object called Calabi- Yau manifold. A 6-dimensional Calabi-Yau manifold leads to the idea of mirror symmetry. The article "From Polygons to String Theory" suggests that we can stud the mirror symmetry by working on reflexive polygons. Each polygon provides us a family of curves. In this project, we will study representative polygons that produce elliptic curves.

Hasse Theorem says that the trace of Frobenius endomorphism of an elliptic curve over finite field $\mathbb{F}_p$, denoted a_p, satisfies the absolute value of a_p is less than or equal to $2\sqrt{p}$. One of well-known results regarding to this theorem is the Sato Tate conjecture. Motivated by the article "Finding meaning in error terms", this project attempts to investigate this conjecture on particular chosen elliptic curves. Our method is using data collected by programing PARI/GP and MAGMA in order to make observations. We shall also have a closer look on the torsion subgroup of Mordell-Weil group of our elliptic curves and a relation between these curves over rational field $\mathbb{Q}$ and their reductions over finite field $\mathbb{F}_p$.

Contents

List of Figures

Dedication

To Me An, for your unconditional love and everything you have done for me. Without you, I could not become who I am today.

Acknowledgments

I would like to thank my advisor Branden Stone for supporting me with his knowledge, encouragement and patience.
I also want to thank John Cullinan and James Belk for their helpful advices.
To my friends Jin Zhang, Van Mai Nguyen Thi, Thinh Pham, “Thank you for their help on editing.”
To my family and friends, whose names are already written in my heart, “Thank you for your constant support. You are always my unlimited source of inspiration. ”

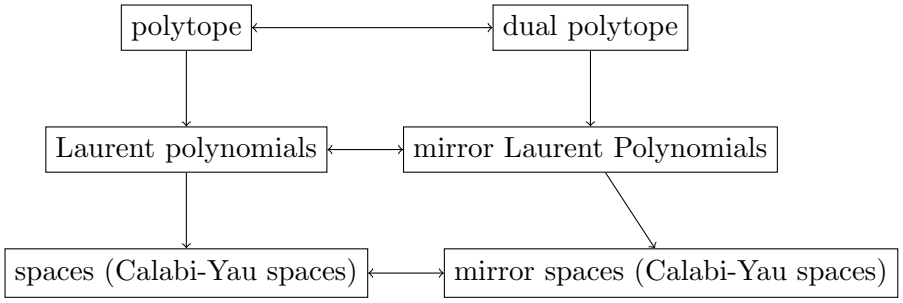
1
Introduction

Human beings are curious by nature. We have been searching thousands years to answer the question "What is the world made of?", "Where and when do things come from?", "When and where do they end?" In Physics, string theory is the most recent theory that attempts to solve those questions with a very different approach: a string!

The world, according to physicist, is made of small particles such as protons, neutrons, electrons, etc. Before string theory, those particles are treated as points in space. The concept of points is so widely used in our daily that we do not usually question of what actually a point is. In Mathematics, a point is actually a fundamental to construct bigger geometric objects such as line, square, cube, etc. Thus, it is quite natural for us to think that our fundamental particles are points. However, string theory says that this is a huge deduction, and those particles should be treated as objects made by strings. At first, this idea is not quite intuitive.However, if we take a closer look we will see that a point can only move, but a string can actually change shape, and that an object made by a string is ultimately not so strange to those studying topology.

We cannot study string theory without mentioning an algebraic geometric object called Calabi-Yau manifold. A 6-dimensional Calabi-Yau is conjectured to be the form of extra dimensions of space-time. Two Calabi-Yau manifolds can be very geometrically different, yet equivalent if they share certain properties in string theory. These two manifolds are called mirror manifolds. This leads us to study mirror symmetry.

Motivated by the idea in [1] that a mirror space in string theory can be studied by studying reflexive polygons (a polygon is 2-dimensional polytope), this project is initially composed for the purpose of comparing a polygon and its dual. Each polygon produces a family of Laurent polynomials. For each family we choose one representative Laurent polynomial, from which we want to construct elliptic curves , and to study similarity as well as differences between the curves that are produced from polygons and their dual. The following diagram taken from [1] shows us briefly the relationship between polytopes and mirror spaces.



The result turns out to be more general than initially thought. All of the elliptic curves produced by reflexive polygons have a lot in common with each other, and therefore, the main results are presented in a group of curves instead of each pair of curves. However, to lead the reader to main results of this project in Chapter 5, we need to introduce three chapters before it. In Chapter 2, we shall go through basic definitions of polytopes and elliptic curves. In this chapter, two new mathematical varieties will be introduced: affine varieties and projective varieties with examples in order to illustrate the concept of elliptic

curve. Chapter 3 is devoted to defining the addition among points on elliptic curve and group law of rational points. Since conjectures of this project are mainly based on the data that are collected by using MAGMA and PARI codes, we shall spend Section 4.2 of Chapter 4 to talk about the codes. Before that, in Section 4.1, we shall discuss how to translate a polygon to an elliptic curve. Chapter 5 presents the main results of this project. Finally, Chapter 6 is our future work and some questions we did not have time to investigate in this project.

2
Notation and Basic Definitions

This chapter contains basic knowledge about polytopes and algebraic geometry that is prerequisite of this project. We first consider polytopes, polygon, and their duality. Next, some background on affine varieties and projective varieties will be introduced as a preparation for understanding elliptic curves. The relationships between polygons and elliptic curves will not be introduced until Chapter 4.

2.1 Polytopes and Polygons

We are familiar with examples of polytopes and polygons in our daily life (a cube, a pyramid, a square, a triangle, etc.). Polytopes in 3D and 2D are easy to describe, but it is not easy to give a rigorous definition, or even imagine a polytope in higher dimensions. Using vectors we can construct an algebraic definition of the polytope as follows.

Definition 2.1.1. Let $\{\vec{v_1}, \vec{v_2}, ..., \vec{v_q}\}$ be a set of points in $\mathbb{R}^k$. The **polytope** with vertices $\{\vec{v_1}, \vec{v_2}, ..., \vec{v_q}\}$, denoted $\triangle$, is the set of points of the form

$$\vec{x} = \sum_{i=1}^{q} t_i \vec{v_i},$$

where the t_i are non negative real numbers satisfying $t_1 + t_2 + ... + t_q = 1$.

$\triangle$

A polytope is called **lattice** if the coordinates of its vertices are integral. A **polygon** is a polytope in 2-dimensional space.

Definition 2.1.2. Given a polytope $\triangle$, a **dual polytope** $\triangle^\circ$ is given by

$$\{(m_1, \ldots, m_k) : (n_1, \ldots, n_k).(m_1, \ldots, m_k) \geq -1 \text{ for all } (n_1, \ldots, n_k) \in \triangle\}.$$

$\triangle$

In this definition the inequality is defined for the sake of consistency with one of our main references [1]. However, in some other texts, instead of greater or equal -1, the reader can find the inequality would be less than or equal 1. This distinction does not make much of a difference. Switching the inequality would negate the coordinates of the points, but the geometric properties of the polytope remind the same.

Now, we have definitions of the polytope and its dual in $\mathbb{R}^k$. The following example will show us how we construct duality in a 2-dimensional space.

Example 2.1.3. Consider the polygon in Figure 2.1.1. The polygon has four vertices $(0, 1), (1, 0), (0, -1)$, and $(-1, 0)$. Let us denote the polygon as $\triangle$. We want to construct its dual, $\triangle^\circ$. Because the polygon is the area bounded by 4 lines that intersects with each

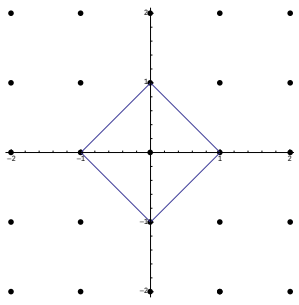


Figure 2.1.1. Polygon example

other at 4 vertices , we see that a point (x, y) is in the polygon if and only it satisfies

$$x - y \geq -1,$$

$$-x - y \geq -1,$$

$$-x + y \geq -1,$$

$$x + y \geq -1.$$

We want to create a polygon from the original polygon. Let us rewrite all in-equations using dot product, then we have the followings:

$$(x, y).(1, -1) \geq -1,$$

$$(x, y).(-1, -1) \geq -1,$$

$$(x, y).(-1, 1) \geq -1,$$

$$(x, y).(1, 1) \geq -1.$$

This implies that $(1, 1), (-1, -1), (-1, 1)$, and $(1, -1)$ are in $\triangle^\circ$ by the definition of duality. Moreover, since the following four equations

$$(x, y).(1, -1) = -1,$$

$$(x, y).(-1, -1) = -1,$$

$$(x, y).(-1, 1) = -1,$$

$$(x, y).(1, 1) = -1.$$

are boundaries of the polygon, four points (1,-1), (-1,-1), (-1,1) and (1,1) are extremal points, Thus, now we can construct the new polygon that has four vertices $(-1, 1), (1, 1), (1, -1)$, and $(-1, -1)$. $\Diamond$

In the example above, we demonstrate how to construct the dual polygon from a given polygon by using equation the edge. This way of constructing can be generalized in a

k-dimensional space. The edge of the polygon is not simply a line, but it is actually a hyperplane of 2-dimensional space (recall from vector calculus, hyperplane of a k-dimensional space is a subspace of $k-1$ dimension).

Let us consider the polytope containing q vertices $v_1, v_2, \ldots, v_q$ in $\mathbb{R}^k$. The polytope is bounded by q hyperplanes,

$$u_{1_1}x_1 + u_{1_2}x_2 + \ldots + u_{1_k}x_k = -1,$$
$$u_{2_1}x_1 + u_{2_2}x_2 + \ldots + u_{2_k}x_k = -1,$$
$$\vdots$$
$$u_{q_1}x_1 + u_{q_2}x_2 + \ldots + u_{q_k}x_k = -1,$$

Then the dual polytopes contains q vertices $\vec{u_1}, \vec{u_2}, \ldots, \vec{u_q}$ where $\vec{u_i} = (u_{i_1}, u_{i_2}, \ldots, u_{i_k})$.

In reality, we notice that not all lattice polytopes have a dual that is also lattice, the dual polytope can have rational vertices, so we have the following definition:

Definition 2.1.4. A lattice polytope $\triangle$ is called **reflexive** if its dual form, $\triangle^\circ$, is also a lattice. $\triangle$

Theorem 2.1.5. *If $\triangle$ is a reflexive polytope, then $(\triangle^\circ)^\circ = \triangle$.*

Proof. By definition of dual polytope, $\triangle^\circ = \{(m_1, \ldots, m_k) : (n_1, \ldots, n_k).(m_1, \ldots, m_k) \geq -1 \text{ for all } (n_1, \ldots, n_k) \in \triangle\}$, we know that every points in $\triangle$ should be in $(\triangle^\circ)^\circ$ as well.

Suppose $T = (t_1, \ldots, t_k)$ is a point that not in $\triangle$. We know that, in $\mathbb{R}^n$ the hyperplane of the form

$$u_{i_1}x_1 + u_{i_2}x_2 + \ldots + u_{i_k}x_k = -1 \text{ where } u_{i_1}, u_{i_2}, \ldots, u_{i_k} \in \mathbb{R}$$

separates the space into two parts, one part contains points that have coordinates $(x_1, \ldots, x_k)$ such that

$$u_{i_1}x_1 + u_{i_2}x_2 + \ldots + u_{i_k}x_k < -1,$$

and the other contains points that have coordinates satisfying

$$u_{i_1}x_1 + u_{i_2}x_2 + \ldots + u_{i_k}x_k \geq -1.$$

By the construction of the dual polytope and its definition, we know that our original polytope is in the second half of the space. Therefore, if $T = (t_1, \ldots, t_k)$ is not in $\triangle$ then T is in the other half of the space, i.e. $u_{i_1}x_1 + u_{i_2}x_2 + \ldots + u_{i_k}x_k < -1$. However, we know that $(u_{i_1}, u_{i_2}, \ldots, u_{i_k})$ is a point in $\triangle^\circ$ by the construction of the dual polytope. This implies that T is not in $(\triangle^\circ)^\circ$.

Thus, we can conclude that $\triangle = (\triangle^\circ)^\circ$.

□

In this project, we will focus on polygons (polytopes in 2-dimension). Next we want to classify reflexive polygons into classes, but then we have to describe reflexive polygons in a different way using the concept of Fano polygon. Even though we cannot list every possible Fano polygon, we can classify them into classes. We will also prove that a reflexive polygon is indeed a Fano polygon. Then, we will classify reflexive polygons.

Definition 2.1.6. A **Fano polygon** is a lattice polygon that contains only the origin in its interior. △

Recall that the definition of the group $\mathbf{GL}(2, \mathbb{Z})$ is the set of matrices $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$, which has determinant is 1 or -1, and a, b, c are all integers.

Definition 2.1.7. We say two Fano polygons $\triangle$ and $\triangle'$ are $\mathbf{GL}(2, \mathbb{Z})-$*equivalent* if there exists a matrix A in $\mathbf{GL}(2, \mathbb{Z})$ such that $\triangle' = \{A \cdot \begin{pmatrix} x \\ y \end{pmatrix} \mid \text{for all } (x, y) \in \triangle\}$. △

Now, using this concept of equivalence, we will compute equivalence classes among Fano polygons. The following lemma is proved in [3].

Lemma 2.1.8. *There are 16 equivalence classes of Fano polygons.*

Theorem 2.1.9 (taken from [1]). *A lattice polygon is reflexive if and only if it is Fano.*

Now, we consider only representatives of each classes. Figure 2.1, notation ↕ denotes duality. We have 20 polygons, but Polygon 12-15 are self-dual. These specific polygons will be our main focus in this project.

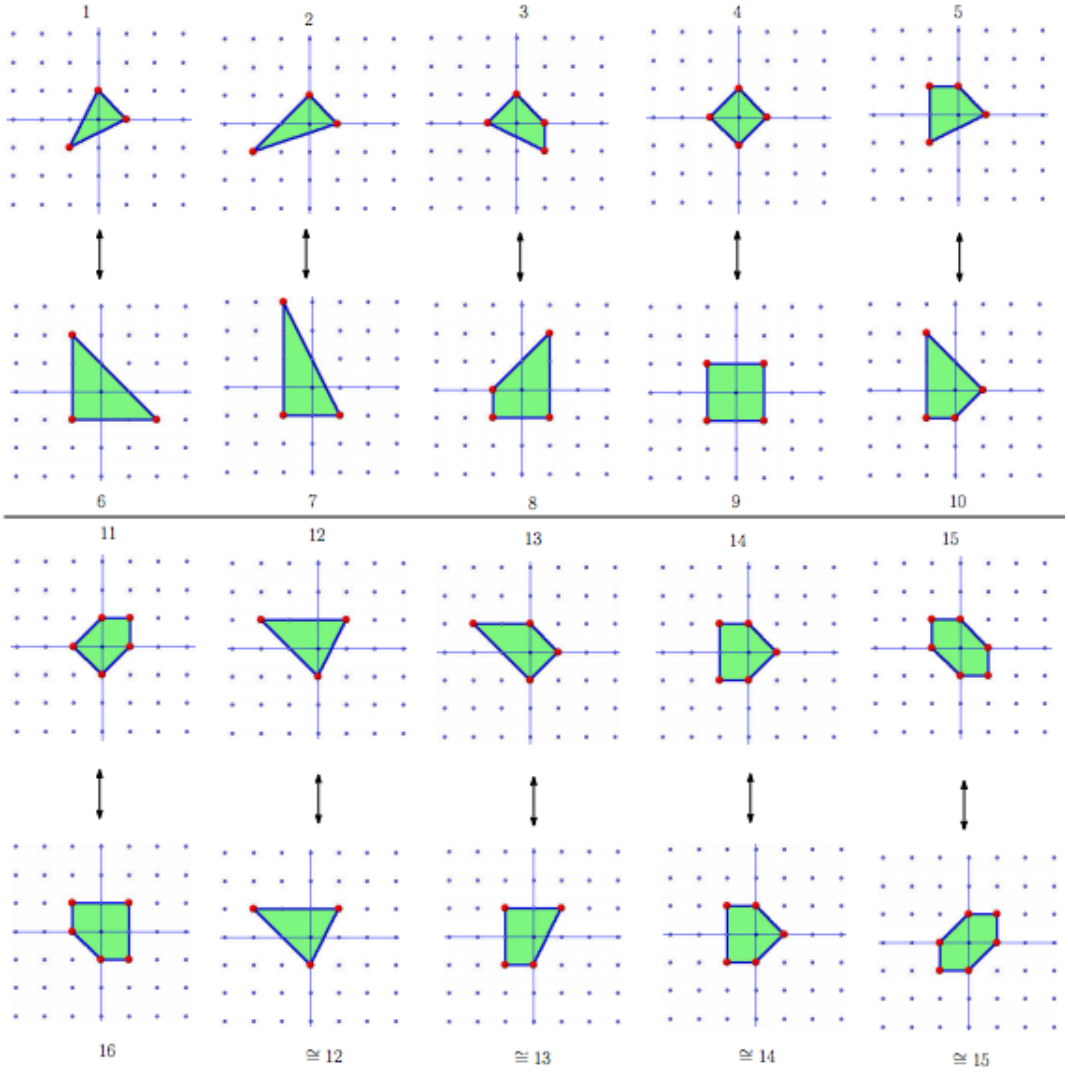


Figure 2.1.2. 16 reflexive polygons as taken from [1]

2.2 Affine Varieties

Before we begin to introduce algebraic geometry, we recall some standard terms in field theory that are used to define later concepts. If there exist fields L, K such that $L \subset K$, and L is closed under the field operations of K and under taking inverses in K, then L is a **subfield** of K, and K is a **field extension** of L.

An element $\alpha \in K$ is said to be **algebraic** over K if it is a root of a polynomial in $K[x]$, otherwise it is **transcendental**.

If every non-constant polynomial in $K[x]$ has a root in K, K is **algebraically closed**. For every field K, if there exists an extension $\overline{K}/K$ such that $\overline{K}$ algebraically closed, then $\overline{K}$ is an algebraic closure of K.

A field K is **perfect** if every irreducible polynomial over K has distinct roots.

From now on, we assume K is a perfect field, and $\overline{K}$ is a fixed algebraic closure of K .The following definitions are taken from [4].

Definition 2.2.1. Affine n-space(over K) is the set of n-tuples

$$\mathbb{A}^n = \mathbb{A}^n(\overline{K}) = \{(x_1, x_2, \ldots, x_n) : x_i \in \overline{K}\}.$$

Similarly, the set of **K-rational points** in $\mathbb{A}^n$ is the set

$$\mathbb{A}^n(K) = \{P = (x_1, \ldots, x_n) \in \mathbb{A}^n; x_i \in K\}.$$

△

Definition 2.2.2. A continuously differentiable curve written in the from $f(x, y) = 0$ is said to be **singular** if there is a point on the curve at which both of the partial derivatives of f are zero. Otherwise, the curve is called **non-singular**. △

Example 2.2.3. Consider two varieties over $\mathbb{R}$

$$A_1 : Y^2 - X^3 = 0,$$

$$A_2 : Y^2 - X^3 - 2X = 0.$$

According to Theorem 2.2.2, we know that any singular points on A_1 must satisfy

$$2Y = 3X^2 = 0.$$

We can easily find out that $(0, 0)$ is a singular point of A_1. Similarly, any singularity points on A_2 must satisfy

$$2Y = 3X^2 + 2 = 0.$$

There is no (X, Y) such that $X, Y \in \mathbb{R}$ and satisfy the equation. Therefore, A_2 is non-singular. $\Diamond$

2.3 Projective Space

To illustrate the importance of constructing projective plane, we borrow the example of Fermat equation from [5]

Example 2.3.1. Consider the solution in rational number of famous Fermat equation,

$$x^N + y^N = 1 \tag{2.3.1}$$

Suppose that $x = \frac{a}{c}$ and $y = \frac{b}{d}$where $c, d > 0$ and $\gcd(a, c) = 1$, $\gcd(b, d) = 1$. Then, we have equation,

$$a^N d^N + b^N c^N = c^N d^N$$

It implies that $c^N \mid a^N d^N$, which means $c^N \mid d^N$ because $\gcd(a, c) = 1$. Similarly, we have $d^N \mid c^N$. Therefore $c = d$ because $c, d > 0$. Thus, the solution of (2.3.1) is $\frac{a}{c}$ and $\frac{b}{c}$. This solution gives us the solution (a, b, c) of the equation

$$x^N + y^N = z^N \tag{2.3.2}$$

Conversely, if $c \neq 0$, the solution (a, b, c) of equation(2.3.2) yields $(\frac{a}{c}, \frac{a}{b})$ as a solution of equation (2.3.1).

Then, we can create map ϕ from set of solutions of equation(2.4.1) to the set of solutions of equation (2.3.1) given by

$$\phi(a,b,c) = (\frac{a}{c}, \frac{b}{c})$$

However, this map is not well-defined yet. $(0,0,0)$ can not be mapped to any solution of the equation (2.3.1). If $a \in \mathbb{Z}$, then $(-a,a,0)$ is a solution of (**??**), but $(\frac{-a}{0}, \frac{a}{0})$ is not defined. Moreover, even if we ignore those special points, this map is not one-to-one because if (a,b,c) is a solution of (2.3.2), then (ta,tb,tc) is also a solution of equation (2.3.2) because they are both mapped to $(\frac{a}{c}, \frac{b}{c})$.

In order to solve these two problems, we construct a new space called projective space.

$\Diamond$

Definition 2.3.2. Projective n-space (over K), denoted $\mathbb{P}^n$ is the set of all $(n+1)$-tuples.

$$(x_0, \ldots, x_n) \in \mathbb{A}^{n+1}$$

such that at least one x_i is non-zero, modulo the equivalence relation given by

$$(x_0, \ldots, x_n) \sim (y_0, \ldots, y_n)$$

if there exists a $\lambda \in \bar{K}^*$ with $x_i = \lambda y_i$ for all i (note that $\bar{K}^* = \bar{K} - \{0\}$).

An equivalence class $\{\lambda x_0, \ldots, \lambda x_n\}$ is denoted $[x_0, \ldots, x_n]$, and $x_0, \ldots, x_n$ and are called **homogeneous coordinates** for their corresponding point in $\mathbb{P}^n$. $\triangle$

Definition 2.3.3. The set of **K-rational points in $\mathbb{P}^n$** is the set

$$\mathbb{P}^n(K) = \{[x_0, x_1, \ldots, x_n] \in \mathbb{P}^n : x_i \in K\}.$$

$\triangle$

Example 2.3.4 (Continue Example 2.3.1)**.** Now if we let solutions of equation (2.3.2) line in projective space, then we can ignore the point $(0,0,0)$. Two points (a,b,c) and (ta,tb,tc) are now considered as one point and is mapped to $(\frac{a}{c}, \frac{b}{c})$.

How about the point of the form $(a, b, 0)$? $(a, b, 0)$ satisfies $a^N + b^N = 0$, $b = -a$. Therefore, we are actually dealing with only two points in $\mathbb{P}^2$, $(-1, 1, 0)$ and $(1, -1, 0)$. Obviously, there is no such a point in the form of $(\frac{1}{0}, \frac{-1}{0})$. However, when the point (a, b, c) goes close to $(-1, 1, 0)$ or $(1, -1, 0)$, the point $(\frac{a}{c}, \frac{b}{c})$ goes to (∞, ∞). This leads to the concept of point at infinity in the set of solutions of (2.3.1). This concept will be studied more in the next chapter. $\Diamond$

2.4 Geometry of Elliptic Curves

Definition 2.4.1. An **elliptic curve (over a field K)** is a smooth (non-singular) projective curve of genus one with a specified point. $\triangle$

Here the genus is defined over the field K and the specified point is a $K - rational$ point .

The definition of a curve requires the definition of genus which is a technical term in topology. Fortunately, for a non-singular curve, we have the degree-genus formula

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

In this project, we will mostly investigate particular cases when the perfect field, K, is either $\mathbb{Q}$ or $\mathbb{F}_p$.

An Elliptic Curve can be written in the form of a homogeneous equation:

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4X^2Z + a_6Z^3$$

with $a_1, a_2, ..., a_6$ are in $\bar{K}$.

From the equation above we can transform it into the form,

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

Such type of equation is called **Weierstrass Equation**.

This transformation either requires Remann- Roch theorem or complicated computations, but we can obtain an intuitive understanding from Silverman's book [5].

When the field K has characteristic different from 2 and 3, then we can simplify the equation into a form

$$E : y^2 = x^3 + ax + b. \tag{2.4.1}$$

The **discriminant** of the curve is defined as $\Delta = -16(4a^3 + 27b^2)$.

The proof of this transformation as well as formulae for elliptic curves over field whose characteristic equal 2 and 3 can be found in [4]. However, we will mostly use equation (2.4.1) in this project.

When the discriminant is different from zero, we can describe points on an elliptic curve using algebraic structure. We can get a different point on the curve by adding two given points.

3
Structure of the group of rational points

In the last chapter we mentioned adding two points on the elliptic curve. In this chapter, we will discuss how we define the addition of points. Defining the addition allows us to form a group of rational points. The structure of this group can be interesting and will be useful in Chapter 5.

3.1 Construct a group of rational points

In this section we focus on the following question: "How do we add two points P and Q on an elliptic curve?"

Consider two distinct points $P = (x_P, y_P)$ and $Q = (x_Q, y_Q)$ on an elliptic curve $y^2 = x^3 + ax + b$ such that $(x_P, y_P) \neq (x_Q, -y_Q)$. We define addition in the following two steps

Step 1

First, we draw a line through P and Q. This line is not a vertical line because $(x_P, y_P) \neq (x_Q, -y_Q)$, we find the third intersection point and denote it $R = P * Q$.

Suppose the line that goes through P and Q is $y = mx + b$. The x-coordinates of three points $P, Q, P*Q$ are solutions of the equation $x^3 + ax + b - (mx + b)^2 = 0$. If this equation

has three distinct solutions, then $P, Q, P * Q$ are three different points. If this equation has only 2 distinct solutions then either $P = R = P * Q$ or $Q = R = P * Q$.

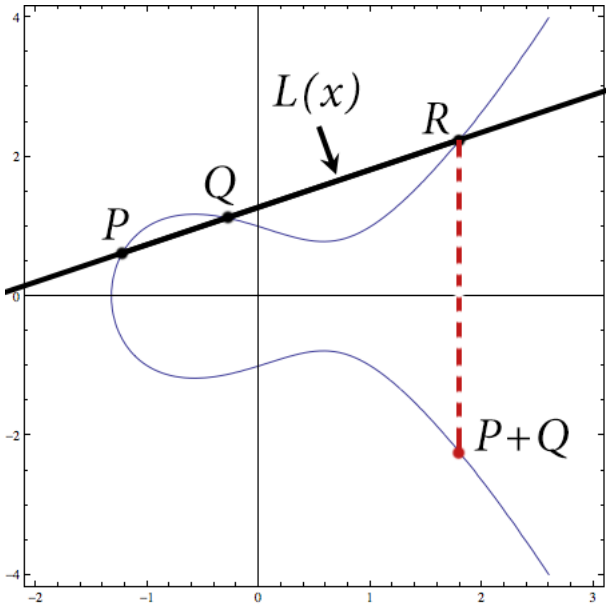


Figure 3.1.1. Adding points example

Step 2

Then we draw the through R and our special (infinity) point $\mathcal{O}$. This line is a vertical line and its second intersection with the curve give us a point, and we call it $P + Q$.

We have defined the addition between P and Q such that $(x_P, y_P) = (x_Q, -y_Q)$. We want to define addition between P and Q when $(x_P, y_P) = (x_Q, -y_Q)$ by using similar steps

Because $(x_P, y_P) = (x_Q, -y_Q)$, the line containing P and Q is a vertical line. The third intersection of this line and the curve is at the point infinity $\mathcal{O}$. Now we have $P * Q = \mathcal{O}$, thus connecting $P * Q$ with $\mathcal{O}$ we will get $P * Q * \mathcal{O} = \mathcal{O} * \mathcal{O} = \mathcal{O}$. Therefore, in this case $P + Q = \mathcal{O}$.

Proposition 3.1.1. *We will prove that this method of defining addition with give us group of a rational points.*

Proof. **Inverterbility**

We have to find the inverse of P, denoted $-P$? As we see above, when $R = (x_P, -y_P)$ we have $P + R = \mathcal{O}$. If P is a rational point, then $R = (x_P, -y_P)$ must be a rational point as well. Therefore, $-P$ exits for all rational point P.

Closure

Suppose $P = (x_P, y_P)$ and $Q = (x_Q, y_Q)$ are rational points on the elliptic curve

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

over the field K.

Then x_P, x_Q are elements of the field K. Consider the cubic equation

$$x^3 + ax + b - (mx + b)^2,$$

where $y = ex + f$ is the line through P and Q, it can be written in the form of $(x - x_P)(x - x_Q)(x - x_{P*Q})$. Since P, Q are rational points, x_P and x_Q are in K, therefor e, x_{P*Q} is also in K. Now, we have $y_{P*Q} \in K$ follows directly. Because $P + Q = (x_{P+Q}, y_{P+Q}) = (x_{P*Q}, -y_{P*Q})$, $P + Q$ is a rational point. Thus, the set of rational points is closed under the addition.

Associativity

In order to prove associativity, I use the following theorem.

Theorem 3.1.2 (Cayley-Bacharach Theorem [2])**.** *Let C, C_1, and C_2 be three cubic curves. Suppose C goes through with of the nine intersection points of C_1 and C_2. Then C goes through the ninth intersection point.*

We know that $P + Q = (P * Q) * \mathcal{O}$. Consider S is another rational point.

$$(P + Q) + S = (P * Q * \mathcal{O}) + S = (P * Q * \mathcal{O}) * S * \mathcal{O}.$$

Similarly, $P + (Q + S) = P * (Q * S * \mathcal{O}) * \mathcal{O}$. Thus, in order to prove we

$$(P + Q) + S = P + (Q + S),$$

we just need to prove that

$$(P * Q * \mathcal{O}) * S = P * (Q * S * \mathcal{O}).$$

Suppose T is the intersection between the line goes through two points $P + Q, S$ and the line goes through $P, Q + S$. We just need to prove that T is on our curve C. Now, we have 9 points $\mathcal{O}, P, Q, S, P + Q, Q + S, P * Q, Q * S$, and T. We can get 3 lines from these 9 points, for example, one line goes through points $P, Q, P * Q$, another goes through points $\mathcal{O}, Q * S, Q + S$, the other goes through points $P + Q, S$. When we multiple these 3 lines we get a cubic curve C_1. Similarly we construct the curve C_2 from 3 different lines that go through 9 points. These two curves are not the same, and they intersect each other at 9 points. Since our curve C contains 8 points, C also contains the ninth points R. □

3.2 Group structure

In the previous section, we proved that rational points on an elliptic curve form abelian group under the defined addition. This group contains elements of both finite and infinite order. Thus, it is natural for us to study elements that have finite orders when we studying the group, especially when it is an abelian group.

Theorem 3.2.1. *Let A be an abelian group. The set containing all elements of finite order, denoted B, is a subgroup of A.*

Proof. It is clear that the identity, denoted e, of A has order 1, so it is contained in B.

Suppose that x of order m and y of order n are two elements of the set B, then we have $e = mx = ny$

We consider $mn(x+y) = (x+y)+(x+y)+\ldots+(x+y)$ (sum of mn numbers of $(x+y)$). Since A is abelian, we can write $mn(x+y) = (x+x+\ldots+x)+(y+y+\ldots+y) = mnx + mny = e + e = e$. This fact implies that the order of $x+y$ is less than or equal mn. Thus, we can conclude that $x+y$ is also of finite order, therefore, $x+y \in B$.

Associativity of B is inherited from A already, so we only care about the invertibility.

Since $x + (m-1)x = mx = e$, the inverse of x is $(m-1)x$. Since x is of finite order, $(m-1)x$ is of finite order as well. Thus, the inverse of x is also in B.

Now, we can conclude B is a group. □

Definition 3.2.2. Let A be an abelian group. The subgroup contains all elements of finite order of A is called **torsion subgroup** of A. △

Definition 3.2.3 (used in Section 5.4)**.** Given an elliptic curve $y^2 = x^3 + Ax + B$. The **division polynomial (torsion polynomial)** are defined

$$\psi_1 = 1,$$
$$\psi_2 = 2,$$
$$\psi_3 = 3x^4 + 6Ax^2 + 12Bx - A^2,$$
$$\psi_4 = 4y(x^6 + 5Ax^4 + 20Bx^3 - 5A^2x^2 - 4ABx - 8B^2 - A^3).$$

We have generalized equation

$$\psi_{2m+1} = \psi_{m+2}\psi_m^3 - \psi_{m-1}\psi_{m+1}^3 \quad \text{where } m \geq 2,$$
$$\psi_{2m} = \frac{\psi_m(\psi_{m+2}\psi_{m-1}^2 - \psi_{m-2}\psi_{m+1}^2}{2y} \quad \text{where } m \geq 3.$$

△

Definition 3.2.4. The **m- torsion subgroup** of E is the set of all points in $E(\bar{K})$ with order m, and is denoted $E[m]$ if and only if mP is the point at infinity (the identity of the group). $\triangle$

The following theorem requires difficult proofs involving complicated technique, so I decided to omit them to focus on the theorem's application.

Theorem 3.2.5. *Suppose that characteristic of the field is k , does not divide m. A point $P = (x, y)$ on E is a root of ψ_m if and only if P is an m torsion point.*

Theorem 3.2.6. [5] *[Nagell- Lutz] Given an elliptic curve $E : y^2 = x^3 + ax + b$, $a, b \in Z$. Let $P = (x, y)$ be a torsion point, $P \neq O$. Then x, y are integers, and $y = 0$ or y^2 divides the discriminant.*

Theorem 3.2.7 (Mazur's Theorem)**.** *Let E be an elliptic curve, the torsion subgroup of $E(\mathbb{Q})$, denoted $(E(\mathbb{Q}))_{tors}$, is isomorphic to group that are one of two forms:*

1. *A cyclic group of order N with $1 < N < 10$ or $N = 12$.*
2. *The product of a cyclic group of order two and a cyclic group of order $2N$ with $1 \leq N \leq 4$.*

4
Computation on Elliptic Curves

4.1 From Polygons to Elliptic Curves

As described in Chapter 2, in 2-dimensional space there are 16 reflexive polygons up to equivalent relations. Each polygon has its own dual polygon (see Figure 2.1).

From these polygons, we can get families of Laurent polynomial. These families of Laurents polynomials will produce family of curves. Each polygons have a dual, and the dual also creates a family of curves. In this project, we only look at cubic curves.

Proposition 4.1.1. *Consider the map*

$$\Phi : \mathbb{Z}^n \longrightarrow K[x_1, x_2, \ldots, x_n]$$
$$\Phi(t_1, t_2, \ldots, t_n) = {x_1}^{t_1} {x_2}^{t_2} \ldots {x_n}^{t_n}.$$

Φ *injective homomorphism.*

Proof. If $(t_1, t_2, \ldots, t_n) \neq (t'_1, t'_2, \ldots, t'_n)$, then there exist at least $i \in [0, n]$ such that $t_i \neq t'_i$. It implies ${x_i}^{t_i} \neq {x_i}^{t'_i}$. Therefore, $\Phi((t_1, t_2, \ldots, t_n)) \neq \Phi((t'_1, t'_2, \ldots t'_n))$. Thus, Φ is

injective

$$\begin{aligned}\Phi((t_1,t_2,\ldots,t_n)+(t_1',t_2',\ldots,t_n')) &= \Phi((t_1+t_1',t_2+t_2',\ldots,t_n+t_n')) \\ &= {x_1}^{t_1+t_1'}{x_2}^{t_2+t_2'}\ldots{x_n}^{t_n+t_n'} \\ &= ({x_1}^{t_1}{x_2}^{t_2}\ldots{x_n}^{t_n}).{x_1}^{t_1'}{x_2}^{t_2'}\ldots{x_n}^{t_n'} \\ &= \Phi((t_1,t_2,\ldots,t_n).(t_1',t_2',\ldots,t_n')).\end{aligned}$$

Therefore, we can conclude that the map Φ is an injective homomorphism. □

Now using the defined map Φ we can map each lattice point in n-dimensional space to on monomial. In order to demonstrate how we get cubic curves from polygons, consider the example below. Notation $\longleftrightarrow$ denotes the injective map.

Example 4.1.2. Using the same polygon as in Example 2.1.3. Its dual polygon is also a lattice polygon as described in the example. This polygon has 5 lattice points, and each point provides a term in a Laurent polynomials.

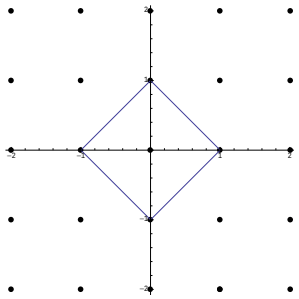


Figure 4.1.1. Polygon example

The followings are lattice points of the polygon and correlative terms in Laurent polynomial

$$(0,1) \longleftrightarrow y,$$

$$(-1,0) \longleftrightarrow x^{-1}y,$$

$$(1,0) \longleftrightarrow x,$$

$$(0,-1) \longleftrightarrow y^{-1},$$

$$(0,0) \longleftrightarrow 1.$$

Then we have a family of Laurent polynomials

$$\alpha_1 x + \alpha_2 y + \alpha_3 x^{-1} + \alpha_4 y^{-1} + \alpha_5 * 1,$$

where α_i is in the field.

If we set the polynomial equal 0, we will have equation,

$$\alpha_1 x + \alpha_2 y + \alpha_3 x^{-1} + \alpha_4 y^{-1} + \alpha_5 * 1 = 0.$$

Multiply both side with xy, we get a cubic

$$\alpha_1 x^2 y + \alpha_2 y^2 x + \alpha_3 y + \alpha_4 x + \alpha_5 xy = 0.$$

Consider the dual polygon in Figure 4.1.2.

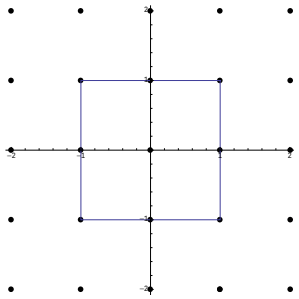


Figure 4.1.2. Polygon example

The followings are lattice points of the polygon and correlative terms in Laurent polynomial.

$$(1,1) \longleftrightarrow xy,$$

$$(1,0) \longleftrightarrow x,$$

$$(1,-1) \longleftrightarrow xy^{-1},$$

$$(0,-1) \longleftrightarrow y^{-1},$$

$$(-1,-1) \longleftrightarrow x^{-1}y^{-1},$$

$$(-1,0) \longleftrightarrow x^{-1},$$

$$(-1,1) \longleftrightarrow x^{-1}y,$$

$$(0,1) \longleftrightarrow y,$$

$$(0,0) \longleftrightarrow 1.$$

We have a family of Laurent polynomials

$$\beta_1 xy + \beta_2 x + \beta_3 xy^{-1} + \beta_4 y^{-1} + \beta_5 x^{-1}y^{-1} + \beta_6 x^{-1} + \beta_7 x^{-1}y + \beta_8 y + \beta_9 * 1.$$

Then, we get the equation,

$$\beta_1 x^2y^2 + \beta_2 x^2y + \beta_3 x^2 + \beta_4 x + \beta_5 + \beta_6 y + \beta_7 y^2 + \beta_8 xy^2 + \beta_9 xy = 0.$$

$\Diamond$

In the example, we only focus on the first polygon because it produces elliptic curve, the second polygon does not. We will investigate particularly curves that has coefficient $\alpha_i = 1$when coefficient α_i is not a free coefficient.

4.2 Coding

Now we get the homogeneous equations from polygons, and I use Magma to get Weierstrass form of these equations.

Using Weierstrass equation that Magma print out, I plug into Pari/GP to find out how many solutions mod p on the curve where p is a prime in the interval $[1, 100000]$.

Motivated Hasse's theorem and Sato conjecture, I used Pari/GP to calculate a_p which is defined by formula $a_p = N_p - p - 1$ where N_p is number of integer solutions on mod p on the curve (p is given).

Theorem 4.2.1 (Hasse's Theorem)**.** *The number of points on a non-singular cubic curve over the finite field F_p is $1 + p + \epsilon$ with $\mid \epsilon \mid < 2\sqrt{p}$.*

Example 4.2.2. I start with the homogenous equation: $x^2y + xy^2 + yz^2 + xz^2 + xyz$. The following is the code in MAGMA. This code actually produces the Weierstrass normal form of the elliptic curve over rational field, i.e $y^2 = x^3 + ax + b$, and the structure of Mordel Weill Group (group of rational points) including the torsion subgroup.

```
PP<x,y,z>:=ProjectiveSpace(Rationals(),2);
C:=Curve(PP, x^2*y+x*y^2+y*z^2+x*z^2+x*y*z);
P0:=C![-1,1,0];
E:=EllipticCurve(C,P0);
WeierstrassModel(E);
MordellWeilShaInformation(E);
```

And Magma will give the result as follows :

```
Elliptic Curve defined by y^2 = x^3 - 27*x + 8694 over Rational Field
Torsion Subgroup = Z/4
Analytic rank = 0
```

```
==> Rank(E) = 0
```

The result shows the Weiestrass normal of form of the elliptic curve, $y^2 + 0xy + 0y = x^3 + 0x^2 - 27x + 8694$. I plug the coefficients into Pari code, to find the discriminant. For each prime $p < 10^5$, this code also provide the trace of Frobenius endomorphism, a_p, as well as the number of solution N_p of the elliptic curve over finite field $\mathbb{F}_{\text{|}}$.

Code 2,

```
Pari: polygon4= ellinit([0,0,0,-27,8694])
Pari: polygon4.disc
Pari: forprime(p=1,100000,print(p,",",1+p-ellap(polygon4,p), ",", (ellap(polygon4,p)))
```

However, sometimes, the Weierstrass normal form has a rational coefficients instead of integral coefficients, thus, the following code is used in order to produce Weierstrass equation

```
Magma:  PP<x,y,z>:=ProjectiveSpace(Rationals(),2);
C:=Curve(PP, x^2*y+y^2*z+x*y^2+x*z^2+z^3+x*y*z+y*z^2);
P0:=C![-1,1,0];
E, phi:=EllipticCurve(C,P0);
Em, psi:= MinimalModel(E);
E;
Em;
Rank(Em);
```

And Magma will give the result as follows :

```
Elliptic Curve defined by y^2 + x*y - y = x^3 + x^2 + x over Rational Field
Elliptic Curve defined by y^2 + x*y + y = x^3 + x^2 over Rational Field
0
```

Then we use this result in Code 2. ◊

5
Results and Conjecture

In this chapter, we will look at elliptic curves that are produced by polygons and their duals (if possible). The curves will be considered over rational field $\mathbb{Q}$ and finite field $\mathbb{F}_p$. We will examine the torsion subgroup of the group of rational points, and the graph that shows the possibility of having $\frac{a_p}{2\sqrt{p}}$ (a_p is the trace of Frobenius endomorphism) in a given interval (a, b) contained in $[-1, 1]$.

5.1 Polygon 1

The first polygon that gives us an elliptic curve is the first polygon in the 20 polygons, we called it Polygon 1. This polygon can be seen in Figure 5.1.1.

The followings is the information that MAGMA and PARI/GP codes provide.

- The lattice points lying in Polygon 1 produces homogeneous equation

$$x^2 * y + y^2 * x + x * y * z + z^3.$$

- Weierstrass normal form of this cubic curve is $y^2 = x^3 - 675 * x + 13662$ over rational field, $\mathbb{Q}$.

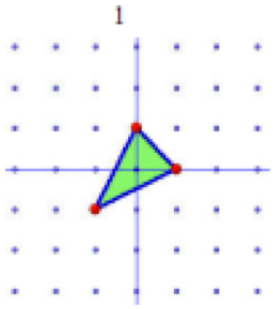


Figure 5.1.1. Polygon 1

- The torsion subgroup of this elliptic curve is isomorphic to $\mathbb{Z}/6$.

- The discriminant of the curve is $\Delta = -60949905408 = -2^{14}3^{12}7$.

By Nagell-Lutz theorem, we know that if $P = (x_P, y_P)$ is the point of order 6, then x_P, y_P are integers and $y_P^2 \mid \Delta$. Thus, y_P can only be multiple of 2 or 3, but cannot be a multiple of 7(if y_P is a multiple of 7, then y_P^2 is a multiple of 49, which implies that y_P^2 does not divides Δ). We use the following code in Pari to find coordinates of P,

```
for(n=0,7,
for(m=0,6, print(m,"   ",n,"   ",factor(x^3-675*x+13662 - 2^(2*n)*3^(2*m))))
)
```

A number whose square divides the discriminant $\Delta = -2^{14}3^{12}7$ is of the form $y = 2^m 3^n$. The above code tries all possibilities of m, n that provide integer x by factor $x^2 - 675x + 13662 - y^2$. According to Pari, there are two cases: $(x, y) = (3, 2^3 3^2)$ or $(x, y) = (39, 2^3 3^3)$.

Function $ellorder(E, z)$ in PARI prints out the order of point z on elliptic curve E. Using the function to check the result, we find out that $P = (39, 2^3 3^3)$ has order 6.

The curve over finite field $\mathbb{F}_p$. Using Code 2, we collect the number of rational points on the elliptic curve and the number a_p for each $p < 10^5$. The following table shows numbers of rational point on the elliptic curve for the first twenty $\mathbb{F}_p$:

p	number of solutions	p	number of solutions
5	6	41	36
7	7	43	36
11	12	47	60
13	18	53	48
17	12	59	66
19	18	61	54
23	24	67	72
29	36	71	72
31	36	73	72
37	36	79	72

Observation. It shown in the table that when p is a good prime, the number of solutions is a multiple of 6. We will prove this observation in Section 5.9.

According to Hasse's Theorem, we know that $\mid a_p \mid 2\sqrt{p}$, which means $-1 \leq \frac{a_p}{2\sqrt{p}} \leq 1$. Thus, we can create a graph that shows the possibilities of a_p in the a particular interval within $[-1, 1]$. In the Figure 5.1.2, each interval has the length of 0.0014.

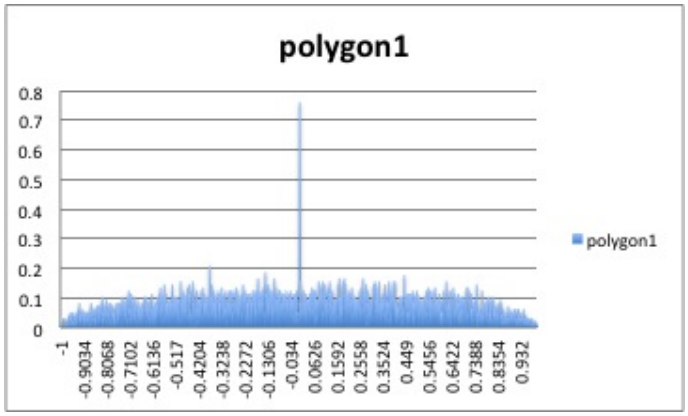


Figure 5.1.2. Polygon 1-The probability of having $\frac{a_p}{2\sqrt{p}}$ in a given interval of length 0.0014

Observation. The Figure 5.1.2 shows that the probability of $\frac{a_p}{2\sqrt{p}}$ close to 0 is especially high (greater than 0.7 percentage). There are two reasons for it.

- There are especially many p such that $a_p = 0$.
- When the value of p increases, p is much greater than a_p. Therefore, $\frac{a_p}{2\sqrt{p}}$ is close to 0.

However, checking the data printed out by PARI, we know that there are 71primes having $a_p = 0$ out of 9592 primes (= 0.74 %).The data also shows that when $a_p = 0$, $p \equiv 5($ mod 6).We will prove this in Section 5.9.

5.2 Polygon 3

The second polygon that gives us an elliptic curve is the third polygon in the 20 polygons, we called it Polygon 3. This polygon can be seen in Figure 5.2.1.

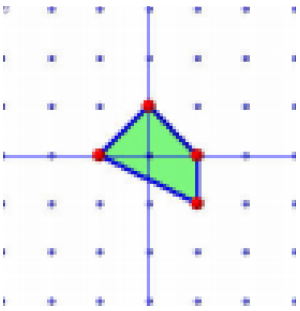


Figure 5.2.1. Polygon 3

Similar to the previous polygon we have the following information about the elliptic curve over rational field produced by polygon 3.

- Homogenous equation is $x^2 * y + x * y^2 + y * z^2 + x^2 * z + x * y * z$.
- Weierstrass normal form is: $y^2 = x^3 - 14256 * x + 279936$.
- The torsion subgroup is isomorphic to $\mathbb{Z}/4$.
- The discriminant of the curve is $\Delta = 2^{24}3^{12}17$.
- Using the discriminant and the same method as we used in polygon 1, we can find the point of order 4, $P = (-36, 2^5 3^3)$.

Now consider the elliptic curve over finite field $\mathbb{F}_p$. The following table shows the numbers of rational point on the elliptic curve for the first twenty $\mathbb{F}_p$.

p	number of solutions	p	number of solutions
5	8	41	48
7	4	43	40
11	12	47	48
13	16	53	48
17	17	59	72
19	24	61	72
23	20	67	64
29	24	71	76
31	28	73	80
37	40	79	68

Observation. It shown in the table that when p is a good prime (i.e. p does not divides the discriminant Δ), the number of solutions is a multiple of 4. We will prove this observation in Section 5.9.

We can also have a graph (see Figure 5.2.2)

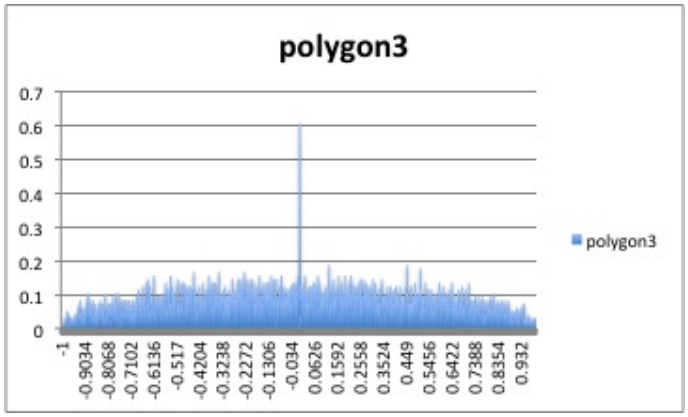


Figure 5.2.2. Polygon 3-The probability of having $\frac{a_p}{2\sqrt{p}}$ in a given interval of length 0.0014

Observation. The Figure 5.2.2 shows that the probability of $\frac{a_p}{2\sqrt{p}}$ close to 0 is especially high (around 0.6 percentage). There are two reasons for it.

- There are especially many p such that $a_p = 0$.
- When the value of p increases, p is much greater than a_p. Therefore, $\frac{a_p}{2\sqrt{p}}$ is close to 0.

However, checking the data printed out by PARI, we know that there are 58 primes having $a_p = 0$ out of 9592 primes (= 0.60 %).The data also shows that when $a_p = 0$, $p \equiv 3($ mod 4).We will prove this in Section 5.9.

5.3 Polygon 4

The third polygon that gives us an elliptic curve is the fourth polygon in the 20 polygons, so we called it Polygon 4. This polygon can be seen in Figure 5.3.1.

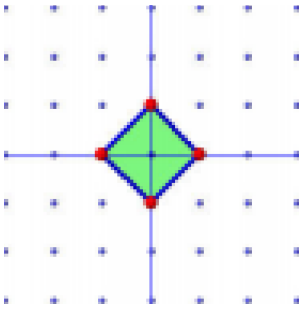


Figure 5.3.1. Polygon 4

Using the same code and argument as we used in polygon 1, we have the following information about the elliptic curve over rational field provided by polygon 4.

- Homogenous equation is $x^2 * y + x * y^2 + y * z^2 + x * z^2 + x * y * z$.
- Weierstrass normal form is: $y^2 = x^3 - 27 * x + 8694$.
- The torsion group of this elliptic curve is isomorphic to$\mathbb{Z}/4$.
- This elliptic curve has $\Delta = -2^{12}3^{13}5$.
- Using this discriminant, we can calculate the point of order 4, $P = (15, 2^2 3^3)$.

Now, let us consider the elliptic curve over finite field, $\mathbb{F}_p$. The following table shows the numbers of rational point on the elliptic curve for twenty $\mathbb{F}_p$.

p	number of solutions	p	number of solutions (N_p)
5	5	41	32
7	8	43	40
11	16	47	40
13	16	53	64
17	26	59	64
19	16	61	64
23	24	67	56
29	32	71	80
31	32	73	64
37	48	79	80

Observation. It shown in the table that when p is a good prime, the number of solutions N_p is a multiple of 8 (so N_p is multiple of 4 as well). We will prove this observation in Section 5.9.

Then we have the following graph,

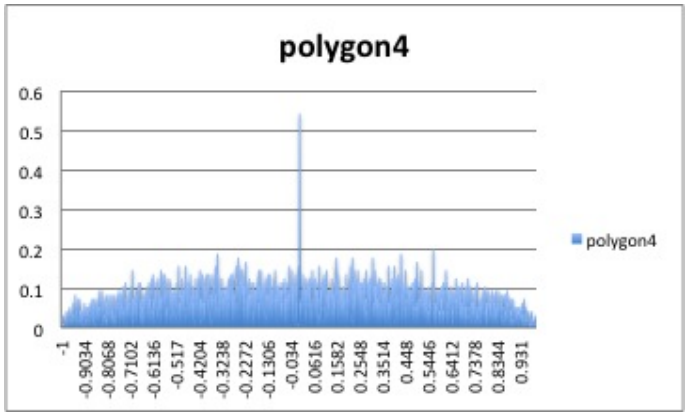


Figure 5.3.2. Polygon 4-The probability of having $\frac{a_p}{2\sqrt{p}}$ in a given interval of length 0.0014

Observation. The Figure 5.3.2 shows that the probability of $\frac{a_p}{2\sqrt{p}}$ close to 0 is especially high (greater than 0.5 percentage). There are two reasons for it.

- There are especially many p such that $a_p = 0$.
- When the value of p increases, p is much greater than a_p. Therefore, $\frac{a_p}{2\sqrt{p}}$ is close to 0.

However, checking the data printed out by PARI, we know that there are 52 p having $a_p = 0$ out of 9592 p (= 0.54 %).The data also shows that when $a_p = 0$, $p \equiv 7(\mod 8)$ or $p \equiv 3(\mod 4)$We will prove this in Section 5.9.

5.4 Polygon 5

The fourth polygon that gives us an elliptic curve is the fifth polygon in the 20 polygons, so we called it Polygon 5. This polygon can be seen in Figure 5.4.1.

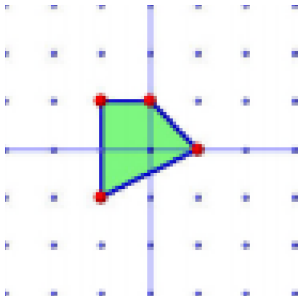


Figure 5.4.1. Polygon 5

Using the same code and argument as we used in Polygon 1, we have the following information about the elliptic curve over rational field provided by Polygon 5.

- Homogenous equation is $x^2 * y + x * y^2 + y * z^2 + x^2 * z + x * y * z$.
- Weierstrass normal form is: $y^2 = x^3 + 6480 * x + 1026432$.
- The torsion group is isomorphic to $\mathbb{Z}$.
- The discriminant of the elliptic curve is $\Delta = -2^{24}3^{12}53$.

According to Nagell theorem, a torsion point different from $\mathcal{O}$ has the square of $y - coordinate$ divides the discriminant. We try every number that has square divides Δ, but none of the cases is the $y - coordinate$ of a torsion point. Thus, we can conclude that the only torsion point on the elliptic curve is $\mathcal{O}$.

Now, consider the elliptic curve over finite field $\mathbb{F}_p$. The following table shows numbers of rational point on the elliptic curve for twenty $\mathbb{F}_p$

p	number of solutions	p	number of solutions
5	6	41	36
7	12	43	46
11	12	47	50
13	17	53	55
17	21	59	62
19	25	61	70
23	17	67	80
29	37	71	71
31	28	73	78
37	33	79	81

Observation. It is shown that the number of solutions N_p is not a multiple of a specific number but 1. Interestingly, we will see that this observation agrees with the observation in Polygon 10, which is its dual.

Then we have the following graph,

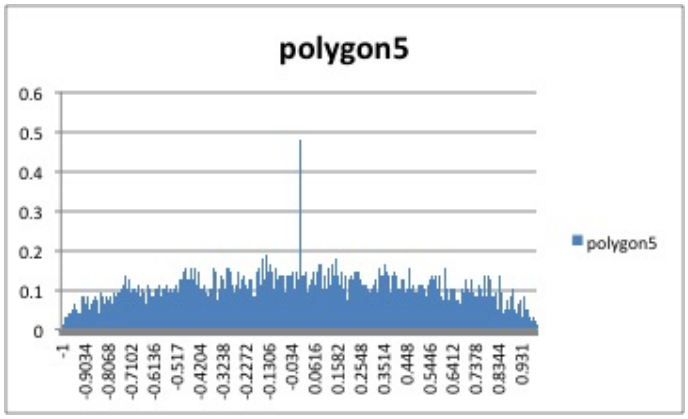


Figure 5.4.2. Polygon 5-The probability of having $\frac{a_p}{2\sqrt{p}}$ in a given interval of length 0.0014

Observation. The Figure 5.4.2 shows that the probability of $\frac{a_p}{2\sqrt{p}}$ close to 0 is especially high (around 0.5 percentage). There are two reasons for it.

- There are especially many p such that $a_p = 0$.

- When the value of p increases, p is much greater than a_p. Therefore, $\frac{a_p}{2\sqrt{p}}$ is close to 0.

However, checking the data printed out by PARI, we know that there are 46 primes having $a_p = 0$ out of 9592 p ($= 0.48$ %).

5.5 Polygon 6

The fifth polygon that gives us an elliptic curve is the sixth polygon in the 20 polygons, we called it Polygon 6. This is the dual of Polygon 1. This polygon can be seen in Figure 5.5.1

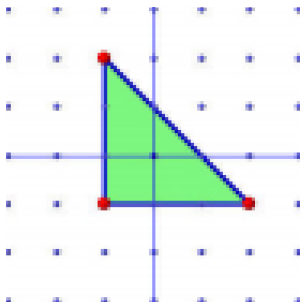


Figure 5.5.1. Polygon 6

Using the same code and argument as we used in Polygon 1, we have the following information about the elliptic curve over rational field provided by Polygon 6:

- Homogenous equation is $y^3+y^2*z+y*z^2+z^3+x*y^2+x*y*z+x*z^2+x^2*y+x^2*z+x^3$.
- Weierstrass normal form is: $y^2 = x^3 - \frac{27}{25} * x - \frac{3186}{625}$ over Rationals field.
- The torsion subgroup is isomorphic to $\mathbb{Z}/3$.

Because the elliptic curve has Weierstrass normal form whose coefficients are not integers, we cannot use Nagel-Lutz Theorem to find a torsion point that generates the torsion subgroup. However, we can use division polynomial to solve this question. According to

theorem 3.2.5, we know that if $P = (x_P, y_P)$ is a 3-torsion point, then x_P is a rational solution of the division polynomial $\psi_3 = 3x^4 - 6 \cdot \frac{27}{25}x^2 - 12 \cdot \frac{3186}{625}x - \frac{27^2}{625}$. The only rational solution of ψ_3 is $x_P = 3$. We plug $x_P = 3$ into the equation $y^2 = x^3 - \frac{27}{25}x - \frac{3186}{625}$ and get $y_P = \frac{-108}{25}$ or $y_P = \frac{108}{25}$. It turns out that both point $(3, \frac{-108}{25})$ and $(3, \frac{108}{25})$ have order 3.

Now consider the elliptic curve. The following table shows numbers of rational points on the curve the first twenty $\mathbb{F}_p$. Since the coefficients of the Weierstrass normal forms has denominators are the power of five, we only consider prime number $p > 5$.

p	number of solutions	p	number of solutions
7	6	43	48
11	15	47	36
13	18	53	48
17	21	59	60
19	15	61	60
23	18	67	81
29	30	71	60
31	30	73	63
37	36	79	90
41	45	83	93

Observation. It shown in the table that when p is a good prime, the number of solutions is a multiple of 3.

Then we have the following graph.

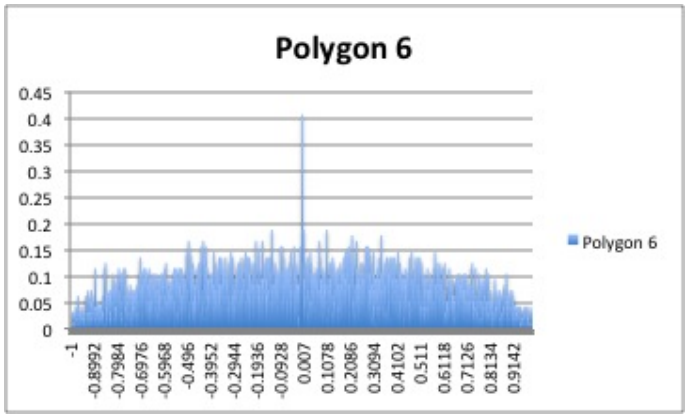


Figure 5.5.2. Polygon 6-The probability of having $\frac{a_p}{2\sqrt{p}}$ in a given interval of length 0.0014

Observation. The Figure 5.5.2 shows that the probability of $\frac{a_p}{2\sqrt{p}}$ close to 0 is especially high (around 0.4 percentage). There are two reasons for it.

- There are especially many p such that $a_p = 0$.
- When the value of p increases, p is much greater than a_p. Therefore, $\frac{a_p}{2\sqrt{p}}$ is close to 0.

However, checking the data printed out by PARI, we know that there are 52 primes having $a_p = 0$ out of 9592 primes (= 0.41 %). The data also shows that when $a_p = 0$, $p \equiv 2(\mod 3)$. We will prove this in Section 5.9.

5.6 Polygon 10

The sixth polygon that gives us an elliptic curve is the tenth polygon in the 20 polygons, so we called it Polygon 10. This polygon can be seen in Figure 5.6.1.

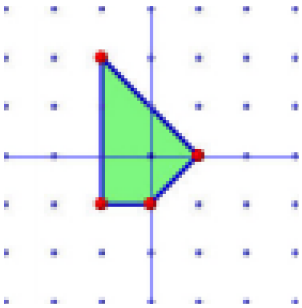


Figure 5.6.1. Polygon 10

Using the same code and argument as we used in Polygon 1, we have the following information about the elliptic curve over rational field provided by Polygon 10:

- Homogenous equation is $x^2 * y + x * y^2 + y^2 * z + z^3 + x * y * z + y * z^2 + y^3 + x * z^2$.
- Weierstrass normal form is: $y^2 = x^3 + 20304 * x - 687744$ over Rationals field.
- The torsion subgroup is isomorphic to $\mathbb{Z}$.

- The discriminant is $\Delta = -2^{24}3^{12}83$.

Now consider the elliptic curve over finite field F_p. The following table shows numbers of rational point on the elliptic curve over the first twenty $\mathbb{F}_p$.

p	number of solutions	p	number of solutions
5	8	41	44
7	11	43	52
11	9	47	48
13	20	53	48
17	13	59	55
19	18	61	57
23	28	67	70
29	37	71	70
31	27	73	74
37	49	79	60

Observation. It is shown that the number of solutions N_p is not a multiple of a specific number but 1. Interestingly, this observation agrees with the observation in Polygon 5, which is its dual.

The we have the following graph,

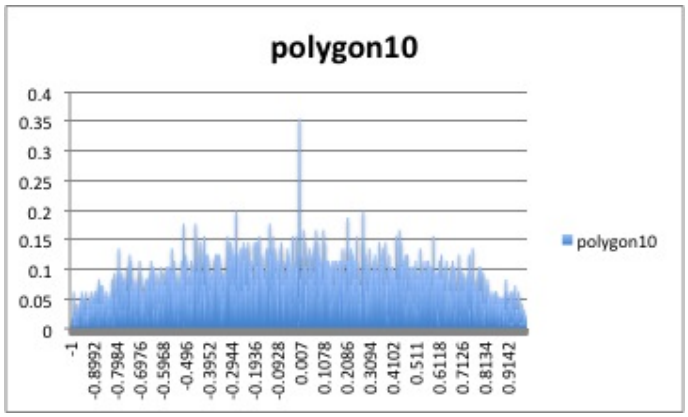


Figure 5.6.2. Polygon 10-The probability of having $\frac{a_p}{2\sqrt{p}}$ in a given interval of length 0.0014

Observation. The Figure 5.6.2 shows that the probability of $\frac{a_p}{2\sqrt{p}}$ close to 0 is especially high (around 0.35 percentage). There are two reasons for it.

- There are especially many p such that $a_p = 0$.

- When the value of p increases, p is much greater than a_p. Therefore, $\frac{a_p}{2\sqrt{p}}$ is close to 0.

However, checking the data printed out by PARI, we know that there are 34 primes having $a_p = 0$ out of 9592 primes (= 0.35 %).

5.7 Polygon 14, 19

The seventh polygon that gives us an elliptic curve is the fourteenth and nineteenth polygon in the 20 polygons, we called it Polygon 14. It is a self dual polygon. This polygon can be seen in Figure 5.7.1.

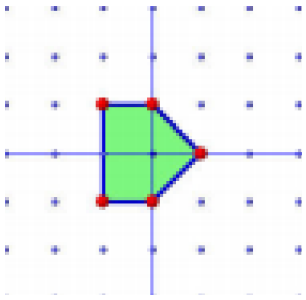


Figure 5.7.1. Polygon 14, 19

Using the same code and argument as we used in polygon 1, we have the following information about the elliptic curve provided by polygon 14:

- Homogenous equation is $x^2 * y + x * y^2 + y^2 * z + z^3 + x * y * z + y * z^2 + x * z^2$.
- Interestingly, this homogenous equation provides the same Weierstrass normal form as the one in Polygon 4, $y^2 = x^3 - 27 * x + 8694$.
- Other information is exactly the same as in Polygon 4.

The following table shows numbers of rational point on the elliptic curve for twenty $\mathbb{F}_p$'s:

p	number of solutions	p	number of solutions
5	5	41	32
7	8	43	40
11	16	47	40
13	16	53	64
17	16	59	64
19	16	61	64
23	24	67	56
29	32	71	80
31	32	73	64
37	48	79	80

Observation. It shown in the table that when p is a good prime, the number of solutions is a multiple of 4.

And we have the following map,

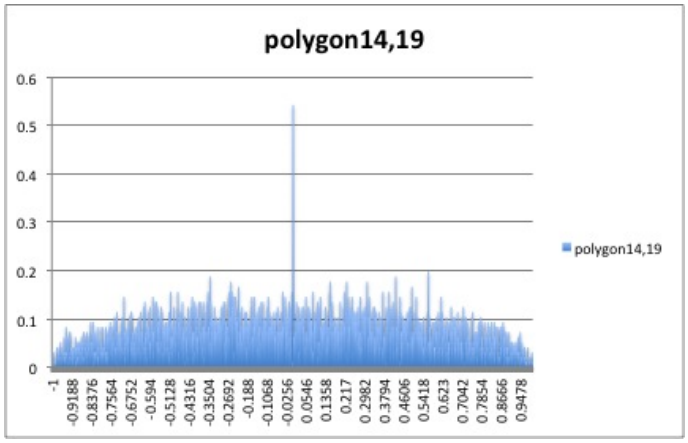


Figure 5.7.2. Polygon 14-The probability of having $\frac{a_p}{2\sqrt{p}}$ in a given interval of length 0.0014

Observation. The Figure 5.7.2 shows that the probability of $\frac{a_p}{2\sqrt{p}}$ close to 0 is especially high (greater than 0.5 percentage). There are two reasons for it.

- There are especially many p such that $a_p = 0$.
- When the value of p increases, p is much greater than a_p. Therefore, $\frac{a_p}{2\sqrt{p}}$ is close to 0.

However, checking the data printed out by PARI, we know that there are 52 primes having $a_p = 0$ out of 9592 primes (= 0.54 %).The data also shows that when $a_p = 0$, $p \equiv 7(\mod 8)$ or $p \equiv 3(\mod 4)$ .We will prove this in Section 5.9.

5.8 Polygon 15

The eighth polygon that gives us an elliptic curve is the fifteenth polygon in the 20 polygons, so we called it Polygon 20. This polygon can be seen in Figure 5.8.1

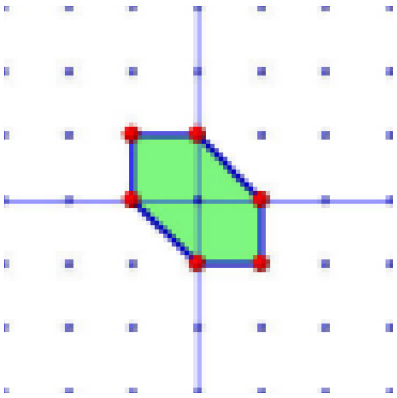


Figure 5.8.1. Polygon 15

Using the same code and argument as we used in polygon 1, we have the following information about the elliptic curve provided by polygon 15.

- Homogenous equation is $y^2 * z + y * z^2 + x * z^2 + x^2 * z + x^2 * y + y^2 * x + x * y * z$.
- Weierstrass normal form is: $y^2 = x^3 - \frac{675}{16}x + \frac{6831}{32}$ over Rationals field.
- The torsion subgroup is isomorphic to $\mathbb{Z}/6$

Since the Weierstrass equation has non-integer coefficients , we cannot apply Nagel-Lutz Theorem in order to find the torsion point generating torsion subgroup.

The following table shows numbers of rational point on the elliptic curve for the first twenty $\mathbb{F}_p$.

p	number of solutions	p	number of solutions
5	6	41	36
7	7	43	36
11	12	47	60
13	18	53	48
17	12	59	66
19	18	61	54
23	24	67	72
29	36	71	72
31	36	73	72
37	36	79	72

Observation. It shown in the table that when p is a good prime, the number of solutions is a multiple of 6.

We have the graph (see Figure 5.8.2)

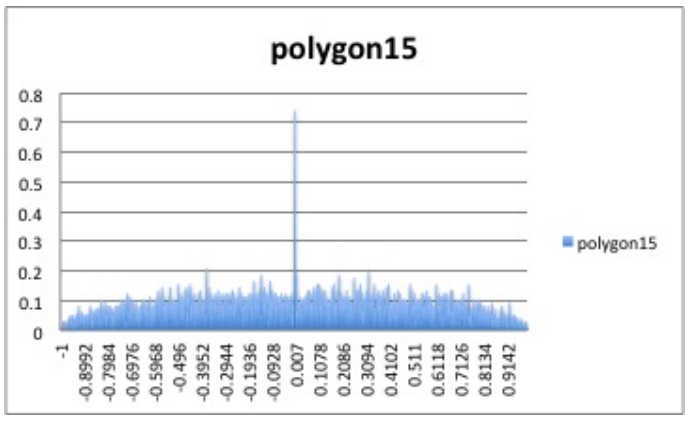


Figure 5.8.2. Polygon 15-The probability of having $\frac{a_p}{2\sqrt{p}}$ in a given interval of length 0.0014

Observation. The Figure 5.8.2 shows that the probability of $\frac{a_p}{2\sqrt{p}}$ close to 0 is especially high (greater than 0.7 percentage). There are two reasons for it.

- There are especially many p such that $a_p = 0$.
- When the value of p increases, p is much greater than a_p. Therefore, $\frac{a_p}{2\sqrt{p}}$ is close to 0.

However, checking the data printed out by PARI, we know that there are 71 primes having $a_p = 0$ out of 9592 primes (= 0.74 %).The data also shows that when $a_p = 0$, $p \equiv 5($ mod 6).

5.9 Points of Finite Order over finite field and over rational field.

We have seen computational results for each polygon in Section $5.1 - 5.8$. In this section, we want to generalize the results and also give explanations for some observations in the previous sections.

The first proposition in this section is a direct application of Mazur Theorem (Theorem 3.2.7).

Proposition 5.9.1. *Let E over rational field $\mathbb{Q}$ be one of elliptic curves in Section 5.1-5.8, then the torsion subgroup of E is isomorphic to $\mathbb{Z}/n$ where $1 \leq n \leq 12$, $n \neq 11$.*

Proof. It is clearly a shown result in Section 5.1-5.8 □

Moreover, from these elliptic curves, we can also easily observe that if the torsion group of an elliptic curve over rational field is isomorphic to $\mathbb{Z}_n$ the number of solutions on elliptic curve over finite fields are multiple of n (except when p is a bad prime). We want to know why there is such a relation. The theorem 5.9.2 will give an answer for this question.

Note that we use $y^2 = x^3 + ax + b$ instead of $y^2 = x^3 + ax^2 + bx + c$ like in [5] for the elliptic curve's equation because the field of rational numbers has characteristic zero.

Theorem 5.9.2 (Reduction Modulo p Theorem [5])**.** *Give an elliptic curve of the Weierstrass equation,*

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

where a, b, c are integers. Let us denote by Δ the discriminant of the curve. Using the map $r : \mathbb{Z} \to \mathbb{F}_p$ where $r(x) = x(\mod p)$, we can construct a new curve:

$$E' : y^2 = x^3 + r(a)x + r(b).$$

If p does not divide 2Δ, then $E(\mathbb{Q})_{tors}$ is isomorphic onto a subgroup of $E'(\mathbb{F}_p)$.

Proof. Let us consider the map $r : \mathbb{Z} \to \mathbb{F}_p$ where $r(x) = x(\mod p)$. Because $r(x) + r(y) = r(x + y) = x + y(\mod p)$, and $r(x).r(y) = r(xy) = xy(\mod p)$, the map is a homomorphism.

Since E has integer coefficient, we can get a new curve, denoted E', that has coefficient in $\mathbb{F}_p$:

$$E' : y^2 = x^3 + r(a)x + r(b)$$

The discriminant of the new curve is $\Delta' = -16(4r(a)^3 + 27r(b)^2)$. However, since the map is a homomorphism, Δ' equal to $r(\Delta)$. Thus, $\Delta' = 0$ when $p \mid \Delta$, and these primes are called bad primes.

We know that points of finite order of elliptic curve E have integer coordinates according to Nagell-Lutz theorem. Suppose $P = (x_P, y_P)$ is a point of finite order, then we have

$$y_P^2 = x_P^3 + ax_P + b.$$

Since r is homomorphism, we can reduce the above equation to

$$r(y_P)^2 = r(x_P)^3 + r(a)r(x_P) + r(b)$$

Thus, the point $r(P) = (r(x_P), r(y_P))$ is on the curve E'. Because E' is over finite field $\mathbb{F}_p$, so we denote $E'(\mathbb{F}_p)$ the group of rational point. Then, we define a map,

$$\phi : E(\mathbb{Q})_{tors} \to E'(\mathbb{F}_p)$$

where $\phi((x, y)) = (r(x), r(y))$ and $\phi(\mathcal{O}) = \mathcal{O}'$. We want to prove that ϕ is an homomorphism.

Let $P, Q, R \in E(\mathbb{Q})_{tors}$. Then, we have

$$\phi(-P) = (r(x_P), r(-y_P)) = (r(x_P), -r(x_P)) = -\phi(P).$$

Suppose $P + Q + R = \mathcal{O}$, so $P + Q = -R$. Then, the statement

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

is equivalent to

$$-\phi(R) = \phi(-R) = \phi(P) + \phi(Q). \tag{5.9.1}$$

Therefore, if we want to prove ϕ is homomorphism, it suffices to prove 5.9.1.

If R is $\mathcal{O}$ then $P = -Q$, that means

$$\phi(P + Q) = \phi(\mathcal{O}) = \mathcal{O}' = \phi(P) - \phi(P) = \phi(P) + \phi(Q).$$

If R is different from $\mathcal{O}$, then let $Q = (x_Q, y_Q)$, and $R = (x_R, y_R)$. Since $P+Q+R = \mathcal{O}$, we know that $P * Q = R$ (recall the notation when we construct the addition among points on elliptic curve). Therefore, P, Q, R are in the same line. Suppose the line going through the three points is

$$y = mx + n.$$

Then we have $m = \frac{y_Q - y_P}{x_Q - x_P}$ and $n = y_P - mx_P = y_Q - mx_Q$.

Because three points P, Q, R are intersections of the line and the elliptic curve, their coordinates are solutions of the equation

$$y^2 = (n + mx)^2 = x^3 + ax + c.$$

Then we can get a cubic equation of x

$$0 = x^3 + ax + c - n^2 - 2mnx - m^2x^2.$$

We know that x_P, x_Q and x_R are three roots of our equation, therefore, we have

$$x^3 - m^2x^2 + (a - 2mn)x + c - m^2 = (x - x_P)(x - x_Q)(x - x_R) \tag{5.9.2}$$

$x^3-m^2x^2+(a-2mn)x+c-m^2 = x^3-(x_P+x_Q+x_R)x^2+(x_Px_Q+x_Qx_R+x_Px_R)x-x_Px_Qx_R.$

From the equation above, we find that $m^2 = x_R + x_P + x_Q$, and we also know that $y_R = mx_R + n$. Because x_P, x_Q, x_R are integers, m and n are integers as well. So now we can reduce the equation (5.9.2) to

$$x^3 - r(m)^2x^2 + (r(a) - 2.r(m)r(n))x + r(c) - r(m)^2 = (x - r(x_P))(x - r(x_Q))(x - r(x_R)).$$

We also have $r(y_R) = r(m)r(x_R) + n$, and $r(y_P) = r(m)r(x_P) + n$. Therefore, we know that $\phi(P), \phi(Q)$, and $\phi(R)$ are intersection the curve $E' : y^2 = x^3 + r(a)x + r(b)$ and the line $y = r(m)x + r(n)$.

Thus, according to how we define the addition among points on elliptic curve we know that $\phi(P) * \phi(Q) = \phi(R)$. This implies that $\phi(P) + \phi(Q) + \phi(R) = \mathcal{O}'$. Then, we can conclude that ϕ is homomorphism.

We have $\phi(x_P, y_P) = (r(x_P), r(y_P))$. If $P \neq \mathcal{O}$, according to Nagel-Lutz Theorem, $y_P \mid \Delta$. Thus, if p is a good prime then, $r(y_P) \neq 0$, then $\phi(P)$ cannot be $\mathcal{O}'$. Therefore, we can say that only $\mathcal{O}$ is mapped to $\mathcal{O}'$. It follows that the kernel of the group homomorphism ϕ is trivial. It implies that ϕ is injective.

We have proved that ϕ is injective homomorphism. This implies $E(\mathbb{Q})_{tors}$ is isomorphic to a subgroup of $E'(\mathbb{F}_p)$. □

The theorem above leads to explanations for our observation in Section 5.1-5.8. These are main results of this project

Corollary 5.9.3. *Let $E : y^2 = x^3 + ax^2 + bx + c$ be an elliptic curve where $a, b, c \in \mathbb{Z}$. Using the map $r : \mathbb{Z} \to \mathbb{F}_p$ where $r(x) = x(\mod p)$, we can construct a new curve,*

$$E' : y^2 = x^3 + r(a)x + r(b).$$

If $E(\mathbb{Q})_{tors}$ is isomorphic to $\mathbb{Z}/n$ then the number of rational points of $E'(\mathbb{F}_p)$ (where $p \neq 2$ or 3, and p does not divides the discriminant) is a multiple of n.

Proof. This proposition is easy to prove by using Theorem 5.9.2. Since $E(\mathbb{Q})_{tors}$ is isomorphic onto a subgroup of $E'(\mathbb{F}_p)$, then $\mid E'(\mathbb{F}_p) \mid$ is a multiple of $\mid E(\mathbb{Q})_{tors} \mid$. Because $E(\mathbb{Q})_{tors}$ is isomorphic to $\mathbb{Z}_n$, we know that the order of the group $E(\mathbb{F}_p)$ is a multiple of n. □

Since we have proved the proposition above, we can confidently claim the following statement.

Proposition 5.9.4. *Suppose N_p is the number of rational points of an elliptic curve E over finite field $\mathbb{F}_p$ for all good primes p we have,*

- *For elliptic curve produced by Polygon 1, N_p is a multiple of 6 (see Section 5.1).*
- *For elliptic curve produced by Polygon 3, N_p is a multiple of 4 (see Section 5.2).*
- *For elliptic curve produced by Polygon 4, N_p is a multiple of 4 (see Section 5.3).*
- *For elliptic curve produced by Polygon 14,N_p is a multiple of 4 (see Section 5.7).*

Unfortunately, in this project, we cannot claim the same thing with elliptic curves that are provided by Polygon 6 and Polygon 15 because they have non-integer coefficients. However, using this statement, wecan partially prove my observation on $a_p = 0$ for elliptic curves constructed from Polygon 1, 3, 4, and 14.

Corollary 5.9.5. *Consider elliptic curve $E : y^2 = x^3 - 675x + 1366$ that is produced by Polygon 1 (see Section 5.1). Let N_p be number of solutions of E over a finite field $\mathbb{F}_p$, and $a_p = p + 1 - N_p$. If $a_p = 0$, then $p \equiv 5(\mod 6)$.*

Proof. According to Proposition5.9.4, we know that $N_p \equiv 0(\mod 6)$. Since $a_p = (p + 1) - N_p$ and $a_p = 0$, we have $N_p = p + 1$. This implies that $p \equiv 5(\mod 6)$. □

Similarly, we can claim that for elliptic curves produced by Polygon 3, 4, and 14 if $a_p = 0$ then $p \equiv 3(\mod 4)$ (see Section 5.2, 5.3, and 5.7).

6
Future work

Chapter 5 shows the datas that we collected and computed. These datas suggest us Proposition 5.9.1 and Corollary 5.9.3 and 5.9.5, which are proved in Section 5.9. However, there are still related questions that need to be solved. In this chapter, we shall spend time to discuss about these questions and further direction for this project.

Question 1 (related to Proposition 5.9.1)**.** Why do all considered elliptic curves in Section 5.1-5.8 have torsion subgroups isomorphic to $\mathbb{Z}/n$ but not to $\mathbb{Z}/2 \times \mathbb{Z}/2N$?

Question 2 (related Corollary 5.9.5 and graphs in Section 5.1-5.8)**.** Why the probability of having $\frac{a_p}{2\sqrt{p}}$ is especially high?

Remark. In the observation of each chapter, I gave out two possible reasons for this questions: it is either because there are especially large number of primes having $a_p = 0$, or because when prime p is very large, $\frac{a_p}{2\sqrt{p}}$ is going to 0.

In the observation, we notice the percentage of primes having exactly $a_p = 0$ is approximately equal to the probability of having $\frac{a_p}{2\sqrt{q}} \approx 0$. This implies that the first argument is more likely the answer than the second argument. If this is the reason, then the question would be "Why there are especially high number of primes producing $a_p = 0$(supersingular

elliptic curve)? However, thinking carefully, it is not necessarily that the number of primes such that $a_p = 0$ is especially high to have the same result as we have. One reason to consider is that when a_p is definitely equal to 0, $\frac{a_p}{2\sqrt{p}}$ is definitely equal to 0, thus, the interval contains 0 has high possibility. However, when $a_p \neq 0$, $\frac{a_p}{2\sqrt{p}}$ is not a fixed number, it can belong to different intervals depends on p.

Question 3. We have proved in Section 5.9 that the elliptic curve produced by Polygon 4 and Polygon 14 has N_p that is multiple of 4 (when p is a good prime), but in the observation N_p is not only a multiple of 4, it is a multiple of 8. Why so?

Question 4. We still have an important question to answer ,"Will this direction give us more specific knowledge about mirror symmetry or only general idea about curve produced by reflexive polygons?"

Remark. Among our 20 polygons, there are only 3 pairs having both the original and the dual polygons produce elliptic curves: Polygon 1 dual with Polygon 6, Polygon 5 dual with Polygon 10, and Polygon 14 is self-dual.

As being seen in Section 5.1-5.8, the torsion subgroup of elliptic curve of Polygon 1 is isomorphic to $\mathbb{Z}/6$, while the elliptic curve of Polygon 6 is isomorphic to $\mathbb{Z}/3$. Both Polygon 5 and 10 produce elliptic curves that have torsion subgroups isomorphic to $\mathbb{Z}$. We some how want to make some relations between the torsion subgroup of curves produced by a polygon and by its dual.

One way to examine this claim is looking the curves that belong to same family by varying coefficients of the curve. The following is an example of Polygon 1 and its dual, Polygon 6.

Example 6.0.6. We consider families of curves that are produced by Polygon 1 and Polygon 6.

Polygon 1

- The family of curve is $\alpha_1 * x^2 * y + \alpha_2 * y^2 * x + \alpha_3 x * y * z + \alpha_4 * z^3$.

- The considered curve has homogenous form

$$x^2 * y + y^2 * x + x * y * z + z^3.$$

  Its Weierstrass form is

$$y^2 = x^3 - 675 * x + 13662.$$

- Now we let $\alpha_1 = \alpha_2 = \alpha_4$ and be equal to 1. We will vary α_3.

  When $\alpha_3 \in \{\frac{1}{2}, \frac{4}{5}2, 3, 7, 12\}$, the torsion subgroups of the curves are isomorphic to $\mathbb{Z}/3$.

- Now we let $\alpha_1 = \alpha_2 = \alpha_3$ and be equal to 1. We will vary α_4.

  When $\alpha_4 \in \{\frac{1}{2}, \frac{4}{5}, 2, 3, 7\}$, the torsion subgroups of the curves are isomorphic to $\mathbb{Z}/3$.

  When $\alpha_4 = 12$, the torsion subgroup of the curve is isomorphic to $\mathbb{Z}/6$.

- Now we let $\alpha_1 = \alpha_3 = \alpha_4$ and be equal to 1. We will vary α_2.

  When $\alpha_2 \in \{\frac{1}{2}, \frac{4}{5}, 2, 3, 7\}$, the torsion subgroups of the curves are isomorphic to $\mathbb{Z}/3$.

  When $\alpha_2 = 12$, the torsion subgroup of the curve is isomorphic to $\mathbb{Z}/6$.

Polygon 6

- The family of curve is

$$\alpha_1*y^3+\alpha_2*y^2*z+\alpha_3*y*z^2+\alpha_4*z^3+\alpha_5*x*y^2+\alpha_6*x*y*z+\alpha_7*x*z^2+\alpha_8*x^2*y+\alpha_9*x^2*z+\alpha_{10}*x^3.$$

- The considered curve has homogenous form

$$y^3 + y^2 * z + y * z^2 + z^3 + x * y^2 + x * y * z + x * z^2 + x^2 * y + x^2 * z + x^3.$$

  Its Weierstrass form is

$$y^2 = x^3 - \frac{27}{25} * x - \frac{3186}{625}.$$

- Now we let $\alpha_i = 1$ where $i \in \{1, 2, \ldots, 10\}$ and $i \neq 4$ We will vary α_4.

  When $\alpha_4 \in \{\frac{1}{2}, \frac{4}{5}2, 7, 12\}$, the torsion subgroups of the curves are isomorphic to $\mathbb{Z}$.

  When $\alpha_4 = 3$, the torsion subgroups of the curve is isomorphic to $\mathbb{Z}$.

$\Diamond$

In the future, we also want to examine other polygons in the same class and their dual polygons to make a further conjecture.

Bibliography

[1] Charles F. Doran and Ursula A. Whitcher, *From polygons to string theory*, Math. Mag. **85** (2012), no. 5, 343–359. MR3007215

[2] David Eisenbud, Mark Green, and Joe Harris, *Cayley-Bacharach theorems and conjectures*, Bull. Amer. Math. Soc. (N.S.) **33** (1996), no. 3, 295–324. MR1376653 (97a:14059)

[3] Benjamin Nill, *Gorenstein toric Fano varieties*, Manuscripta Math. **116** (2005), no. 2, 183–210. MR2122419 (2005k:14110)

[4] Joseph H. Silverman, *The arithmetic of elliptic curves*, Graduate Texts in Mathematics, vol. 106, Springer-Verlag, New York, 1992. Corrected reprint of the 1986 original. MR1329092 (95m:11054)

[5] Joseph H. Silverman and John Tate, *Rational points on elliptic curves*, Undergraduate Texts in Mathematics, Springer-Verlag, New York, 1992. MR1171452 (93g:11003)