ELLIPTIC CURVES

RAHMA SALAMA

Abstract. An elliptic curve is a smooth and unswerving algebraic curve with genus one (roughly definition, curve with one hole in a surface). This special curve captures our attention as we aim to understand its shape and structure when examined across arbitrary algebraically closed fields.

Contents

1. Introduction

In this project, we relay mostly on lecture notes of Kramar without going deeply into the basic concepts that we experienced in the course. We need just to recall some basic definitions and notations from the class note. We start the first section by looking at elementary geometric concepts that we need to define the elliptic curve, then after we proved that every elliptic curve has Waierstrass equation, and we end up by an old application to the elliptic curve.
Let k be a field. We define points in the two-dimensional affine plane, denoted by $\mathbb{A}^2$, over the field k as

$$\mathbb{A}^2 = \{(x, y) \in k \times k\}$$

While the points in the two-dimensional projective space $\mathbb{P}^2$ over the field k, to be the equivalence classes of $(w, x, y) \in \mathbb{A}^3$ such that at least one of w, x, y nonzero, the equivalence class of the point (w, x, y) is

$$[w : x : y] = k^* \cdot (w, x, y) \in \mathbb{P}^2.$$

If the representative point (w, x, y) with $w \neq 0$ then $(w, x, y) = (1, x/w, y/w)$, representing the finite points in $\mathbb{P}^2$. However, if $w = 0$, dividing by w causes a problem of ∞ in either the x or y coordinate, and therefore points $(0, x, y)$ are called the points at infinity in $\mathbb{P}^2$.
Thus, we have a natural embedding

$$\mathbb{A}^2 \hookrightarrow \mathbb{P}^2$$
$$(x, y) \mapsto (1 : x : y)$$

In this way, the two-dimensional affine plane is identified with the finite points in $\mathbb{P}^2$, and adding point at infinity to obtain $\mathbb{P}^2$ can be viewed as a way to compactify the plane. We simply recall the definition in the two-dimensional plane because there is no need for generalization.

By an *affine hypersurface* cut out by a polynomial $f \in k[x_1, \ldots, x_n]$ of degree d over a field k, we mean the collection of vanishing locus $V(f)(K) \subset \mathbb{A}^n(K)$, where K is an extension field, and for $n = 2$ we call $V(f) = C_f \subset \mathbb{A}^2$ an affine plane curve. Similarly, the *projective hypersurface* cut out by a homogeneous polynomial $f \in k[x_0, \ldots, x_n]$ of degree d is the collection of vanishing locus $V(f)(K) \subset \mathbb{P}^n(K)$ and for $n = 2$ we call $V(f) = C_f \subset \mathbb{P}^2$ a plane curve. We also have a bijection that helps to pass between projective and affine hypersurfaces

$$\mathbb{A}^n(K) \to \mathbb{P}^n(K) \setminus V(x_0)(K),$$
$$(a_1, \ldots, a_n) \mapsto (1 : a_1 : \ldots : a_n)$$

So, for any projective hypersurface $V(f) \subset \mathbb{P}^n$ cut out by a homogeneous polynomial $f \in k[x_0, \dots, x_n]$ we get the affine hypersurface $V(f^\flat) \subset \mathbb{A}^n$ cut out by $f^\flat$, the dehomogenization of the polynomial f, where

$$f^\flat(x_1, \dots, x_n) = f(1, x_1, \dots, x_n) \in k[x_1, \dots, x_n]$$

Conversely, we can obtain the projective hypersurface $V(g^\sharp) \subset \mathbb{P}^n$ from the affine hypersurface $V(g)$ cut out by a polynomial $g \in k[x_1, \dots, x_n]$ of degree d, by

$$g^\sharp(x_0, \dots, x_n) = x_0^d \cdot g(\frac{x_1}{x_0}, \dots, \frac{x_n}{x_0}) \in k[x_0, \dots, x_n].$$

2. The plane curves

The compactification of an affine space helps to define the curve generally as a projective variety of dimension one (the dimension of the variety). The projective plane which has extra points at infinity help to understand the geometry of the curves.
Suppose

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

a general cubic equation in x, y and coefficients from the field of definition. A geometric principle can be employed to discover the solution to the cubic equation. When two rational points on a non-singular plane curve are identified, it is generally possible to determine the third point, this is what Mordell (1922) stated. In this section, we aim to outline fundamental geometric ideas and characteristic essential for grasping the concept of Mordell.
The **multiplicity** of the curve at a point? For instance, consider a curve $C : f(x, y) = 0$ and a line $l : y = mx+b$, the x-coordinates of the points of intersection the curve with the line satisfy the equation $g(x) = f(x, mx+b) = 0$ if g does not vanish then it has finite degree. If $p = (a, b)$ is an intersection point then $g(a) = 0$ so we can write $g(x) = (x - a)^m h(x)$ for some polynomial $h(a) \neq 0$ and we say that l intersects the curve at p with multiplicity m.
Another definition of multiplicity will come cross. However, in all cases using the notion of multiplicity we can determine the smoothness of the curve. Let C_f an affine curve, a point $p \in C_f(\overline{k})$ if and only if the multiplicity of the curve at p, denoted by $m_p(C_f) > 0$, and we say p is *smooth* point of C_f if $m_p(C_f) = 1$ and it is *singular* if $m_p(C_f) > 1$. The affine curve C_f is a *smooth* curve if all points $p \in C_f(\overline{k})$ are smooth, and for the projective curve the smoothness property hold if the curve smooth on each affine chart. The affine curve $y - x^2$ is a simply example of the smooth curve where the multiplicity of the curve at $p = (0, 0)$ is 1, and an examples of singular curves are $y^2 = x^2(x - 1)$ and $y^2 = x^3$ the node and cusp (respectively) where the multiplicity of the curve at $p = (0, 0)$ is 2.

Now we want to define the tangent to a plane curve at a given point to understand what is called the order of tangency.

Definition 2.1. Let p be a point on a variety X. By choosing an affine neighborhood of p we assume that $X \in \mathbb{A}^n$ and $p = 0$ is the origin. The vanishing locus of the lowest degree terms

$$T_pX = V(f_d) \subset \mathbb{A}^n$$

, where $f_d \in k[x_1, \dots, x_n]$ denote the linear term of a polynomial $f \in k[x_1, \dots, x_n]$, is the tangent space of X

For the elliptic curve as a smooth curve, assuming it is defined by a polynomial f with no multiple factors over the algebraic closure of the base field, the tangent space equals the tangent line at the point $p \in C_f$. The *order of tangency* of the line l and the curve $C_f \in \mathbb{P}^n$ at the point $p = [w_0 : x_0 : y_0]$ is the vanishing order, and denoted by,

$$i_p(l, C_f) = ord_{t=0}(\varphi(t))$$

where

$$\varphi : \mathbb{A}^1 \to \mathbb{P}^2, t \mapsto [(w_0 + tw_1) : (x_0 + tx_1) : (y_0 + ty_1)]$$

for $q = [w_1 : x_1 : y_1] \in l(k) \setminus p$. Note that $i_p(l, C_f) > 0$ if and only if $p \in (l \cap C_f)(k)$.
Two curves C_1 and C_2 of degree m and n, respectively, meet in mn points, this is what *Bezout's* theorem stated,, and it is follow from the following

Problema 2.2. If $f, g \in k[x, y]$ are polynomials of degree $m, n > 0$, without common factors, then

$$| (C_f \cap C_g)(\overline{k}) | \leqslant dim_k k[x, y]/(f, g) \leqslant mn$$

In the second inequality $'='$ holds unless C_f and C_g intersect at infinity.

The elliptic curve and its group law. We can define now the elliptic curve E as a smooth cubic curve over a field k with point at infinity, denoted by $\mathbf{O}$ or ∞, forming an additive group $(E,+)$. The group law will be constructed geometrically using lines connecting points.

Lemma 2.3. *For any cubic polynomial $g(x) \in k[x]$ without multiple roots in $\overline{k}$ we have the elliptic curve $E \in \mathbb{P}^2$ is the cubic defined by $f^\flat(x,y) = f(1,x,y) = y^2 - g(x)$, and the point at infinity $\boldsymbol{O} = [0:0:1] \in E$ where vertical lines meet, and it is a flex point of the cubic.*
NOTE: *The flex point of the curve is a smooth point where the tangent intersects with a higher order of tangency.*

Proof
The smoothness of E is checked on the ordinary affine plane $\mathbb{A}^2 \in \mathbb{P}^2$ with coordinate $(x,y) = [1:x:y]$, and the system of equations

$$f(1,x_0,y_0) = \frac{\partial}{\partial x} f(1,x_0,y_0) = \frac{\partial}{\partial y} f(1,x_0,y_0) = 0$$

has no solution $(x_0,y_0) \in \mathbb{A}^2(\overline{k})$ since otherwise we would have $g(x_0) = g'(x_0) = 0$ which contradict the assumption that $g(x)$ without multiple root in $\overline{k}$. In the homogeneous coordinates $E \in \mathbb{A}^2$ is the zero locus of $f(w,x,y) = y^2w - x^3 - ax^2w - bxw^2 - cw^3$ with coefficients from k, hence putting $w = 0$ so the only point at infinity is $\mathbf{O} = [0:0:1]$ because $[0:0:0] \notin \mathbb{P}^2$. One easily can checks that the point $\mathbf{O}$ is smooth point by looking at the partial derivative $\frac{\partial}{\partial w} f(0,0,1)$ which is not zero, and the tangent line to E at this point meet the curve with multiplicity three and that proves $\mathbf{O}$ is a flex point.
The group law for elliptic curve involves the composition low which allow to add points, and with the point $\mathbf{O}$ as the identity element this makes the set of points of the elliptic curve into a group. The fact that adding three different points in the curve $P + Q + R = \mathbf{O}$ if and only if they are colinear, the following theorem defines the group operation but the prove will be explained geometrically.

Theorem 2.4. *Let $(E, \boldsymbol{O})$ be an elliptic curve over k. Then for any field K/k the composition law*

$$+ : E(K) \times E(K) \to E(K)$$
$$P + Q \mapsto \boldsymbol{O} * (P * Q)$$

makes $E(K)$ into an abelian group whose neutral element is the point $\boldsymbol{O} \in E(K)$.

By general convention, the points on the cubic consist of the ordinary points in the ordinary affine xy-plane together with additional point $\mathbf{O}$. Thus, to define the addition in the cubic curve we have to know that a line generally meet the cubic in three points, so to add P and Q we draw a line through them and take the third intersection point $P * Q$ and join it to $\mathbf{O}$ by a line, so the third intersection point is $\mathbf{O} * (P * Q)$ which is $P + Q$. And it is clear that this operation is commutative
As the cubic curve is symmetric around x-axis, the negative of the point P is the reflected point $-P$, so the third intersection point when adding P and $-P$ will be $\mathbf{O}$ and connecting $\mathbf{O}$ to $\mathbf{O}$ gives the line at infinity, which is prove that the third intersection is $\mathbf{O}$. Therefore $P + (-P) = \mathbf{O}$.
Let P, Q and R points on the curve, to prove that $(P + Q) + R = P + (Q + R)$ we perform the point addition for P and Q as before. To add $P + Q$ to R, we draw the line through $P + Q$ that meet the curve at $(P + Q) * R$ after that joining $(P + Q) * R$ to $\mathbf{O}$ to get the third intersection point $(P + Q) + R$. For the right hand side we repeat the process starting from adding Q and R to get $Q * R$ and join it to $\mathbf{O}$ and take the third intersection point, which is $Q + R$. Then we must join $Q + R$ to P which gives the point $P * (Q + R)$ and that is suppose to be the same as $(P + Q) * R$. The figure 2 illustrate the group law supposing that $\mathbf{O}$ sitting at the top of the y-axis.

3. Generalized Waierstrass equation

Definition 3.1.

- The local ring of the affine plane at $P = (x_0, y_0) \in \mathbb{A}^n$ is defined by

$$\mathscr{O}_{\mathbb{A}^2,P} = \{\frac{u}{v} \in \overline{k}[x,y] \mid u, v \in \overline{k}[x,y], v(P) \neq 0\}$$

  and its unique maximal ideal is $m_P = \{\frac{u}{v} \in \overline{k}[x,y] \mid u(P) = 0 \neq v(P)\}$
- If $f, g \in k[x,y]$ have no common factor, then for $P \in \mathbb{A}^2(\overline{k})$ we define the multiplicity

$$i_P(f,g) = dim \mathscr{O}_{\mathbb{A}^2,P}/(f,g)_P$$

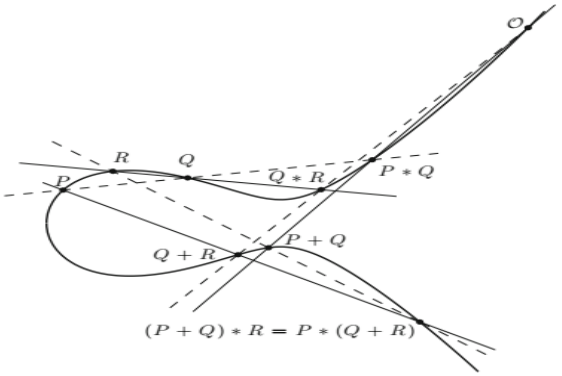

FIGURE 1. Group law: adding points and the associative law

Let the plane curve $C = C_f \subset \mathbb{P}^n$ cut out by an irreducible homogeneous polynomial $f \in k[w, x, y]$ and let $f^\flat \in k[x, y]$ be dehomogenization of f, then $k[x, y]/(f^\flat)$ is an integral domain whose quotient field

$$k(C) = Quot(k[x, y]/(f^\flat))$$

this field is called the *function filed* of the curve and its elements are called rational functions on the curve, and it could be define over the algebraic closure of the base field. In terms of homogeneous polynomials the function field can be written as the residue field $k(C) = \mathscr{O}_{\mathbb{P}^2,C}/(f)$ of the local ring

$$\mathscr{O}_{\mathbb{P}^2,C} = \{g/h \in k(w, x, y) \mid deg(g) = deg(h), f \nmid h\}$$

Definition 3.2. Let $C \subset \mathbb{P}^n$ be a smooth curve, if we have a homogeneous polynomials $g, h \in k[w, x, y]$ and $F = (g/h)|_C \in k(C)^*$ is a rational function other than zero function, we define its order of zeroes or poles at $P \in C(k)$ by

$$ord_P(F) = i_P(f, g) - i_P(f, h)$$

where:

- $ord_P(F) > 0$.
- For any g, h with $F = (g/h)|_C$ we have $g^\flat \in (f^\flat, h^\flat)_P \subseteq \mathscr{O}_{\mathbb{A}^2,P}$.
- There exist $\tilde{g}, \tilde{h}$ with $F = (\tilde{g}/\tilde{h})|_C$ such that $\tilde{h}(p) \neq 0$.

Generally, If $ord_P(F) > 0$, then F has a zero at P , and if $ord_P(F) < 0$, then F has a pole at P. If $ord_P(F) \geq 0$, then F is regular (or defined) at P and we can evaluate $F(P)$.

Problema 3.3. Let C be a smooth curve and $f \in k(C)$ with $f \neq 0$. Then, there are only finitely many points of C at which f has a pole or zero. Further, if f has no poles, then f is constant function.

The following example explain the idea of the order of vanishing at a point:

Example 3.4. Let $f(1, x, y) = y^2 - \varphi(x)$ for a cubic polynomial $\varphi(x) = x^3 + ax + b \in k[x]$ without multiple roots, and we want to compute the order of vanishing (poles) of a rational functions at $P = [0, 0, 1]$, the homogenization form is $f(w, x, y) = y^2w - x^3 - axw^2 - bw^3$ and we can assume that the curve cut out by $f(w, x, y)$ intersects the affine chart when $y = 1$. Therefore, our rational functions are $\frac{x}{w}|_{C_f}$ and $\frac{y}{w}|_{C_f}$. To compute their poles we have to know the dimension of the residue field for each one, to do so we try to compute the intersection multiplicity at P

$$i_P(f, x) = dim\mathscr{O}_{\mathbb{A}^2,P}/(f, x)_P = k[w, x]/(f(w, x, 1), x) \simeq k$$

as the residue field contain the constant functions so the dimension is 1. Similarly

$$i_P(f, w) = dim\mathscr{O}_{\mathbb{A}^2,P}/(f, w)_P = k[w, x]/(f(w, x, 1), x) \simeq k[x]/(x^3)$$

and the dimension of this field is 3, $i_P(f, y) = 0$ since $y \neq 0$ at P. Therefore,

$$ord_P(\frac{x}{w}|_{C_f}) = i_P(f, x) - i_P(f, w) = -2, ord_P(\frac{y}{w}|_{C_f}) = i_P(f, y) - i_P(f, w) = -3$$

3.1. Divisor.

Definition 3.5. A divisor on a smooth plane curve $C \subset \mathbb{P}^n$ is a finite formal sum of points over $\overline{k}$

$$D = \sum_{p \in C(\overline{k})} n_P \cdot [P]$$

where $n_P \in \mathbb{Z}$ and $n_P = 0$ for all but finitely many $P \in C$.

The degree of the divisor D defined by

$$degD = \sum_{P \in C} n_P$$

Let $Div(C)$ denote the abelian group of divisors (it is a free abelain group so we can have infinite sum). The divisors of degree 0 form a subgroup of $Div(C)$ which denoted by $Div^0(C)$, we can also associate a divisor $div(f)$ to a polynomial $f \in \overline{k}(C)^*$ given by

$$div(f) = \sum_P ord_P(f)(P)$$

A divisor $D \in Div(C)$ is principle if $D = div(f)$ for some $f \in \overline{k}(C)^*$. Two divisors D_1, D_2 are linearly equivalent over k, written $D_1 \sim D_2$ if their difference is principle.

Example 3.6. In the previous example we can factor the cubic and get the curve $C : y^2 = (x-r_1)(x-r_2)(x-r_3)$ for distinct root r_1, r_2, r_3, so knowing zeroes and poles of the rational function $x - r_1$ at $p_1 = (1, r_1, 0)$ and at $\mathbf{O} = [0, 0, 1]$ will help to define $div(x - r_1) = 2(p_1) - 2(\mathbf{O})$ and $deg(div(x - r_1)) = 0$

The map $div : k(C)^* \to Div^0(C)$ that sends a rational function to its divisor of zeroes is a homomorphism, with image is the subgroup of *principal divisors* denoted by $PDiv(C)$. The divisor class group (or Picard group) of C, denoted by $Pic(C)$, is the quotient of $Div(C)$ by its subgroup of principal divisors.

Problema 3.7. Let C be a smooth curve and let $f \in \overline{k}(C)^*$.

(a) $div(f) = 0$ if and only if f is constant function.
(b) $deg(div(f)) = 0$

As a consequence, $PDiv(C) \subseteq Div^0(C)$ and we have

$$Pic^0(C) = \frac{Div^0(C)}{PDiv(C)}$$

Definition 3.8. For a curve C, $D \in Div(C)(k)$, the space of rational functions with poles bounded by D is

$$\mathscr{L}(D) = \{f \in k(C)^* \mid div(f) \geq -D\}$$

and we denote its dimension by $l(D) = dim_k \mathscr{L}(D)$

As we define, the space gives us information about the poles of function at a point P. Suppose we have $D = (\mathbf{O})$ and f such that $div(f) \geqslant -(\mathbf{O})$ that means $div(f) + (\mathbf{O}) \geqslant 0, \Rightarrow \sum_{P \neq \mathbf{O}} n_P(P) + (n_{\mathbf{O}} + 1)(\mathbf{O}) \geqslant 0$ that means $n_P \geqslant 0, \forall P \neq \mathbf{O}$ so no poles at $P \neq \mathbf{O}$ and $n_{\mathbf{O}} \geqslant -1, \forall P = \mathbf{O}$ and so there is a pole at $\mathbf{O}$ of order at most 1.

Theorem 3.9. *(Riemann-Roch theorem) Let C be a smooth curve and let K_C be a canonical divisor on C. There is an integer $g > 0$, called the genus of C, such that for every divisor $D \in Div(C)$,*

$$l(D) = deg(D) + 1 - g + l(K_C - D)$$

A clear and detailed prove for the theorem and the following corollary that leads to the consequence in case of elliptic curve in 4.

Corollary 3.10. (a) $l(K_C) = g$.
(b) $deg(K_C) = 2g - 2$.
(c) *If $deg(D) > deg(K_C)$ then $l(D) = deg(D) - g + 1$*

Therefore, in case of elliptic curve with $g = 1$ the version of the theorem becomes

$$l(D) = deg(D), if deg(D) > 0$$

3.2. Waierstrass normal forms. We must establish mappings between curves, enabling the utilization and exchange of properties between them, by using the RiemannRoch theorem we can show that every elliptic curve can be written as a plane cubic, and conversely, every smooth Weierstrass plane cubic curve is an elliptic curve.

Definition 3.11. Consider the plane curve $C_f \subset \mathbb{P}^2$ cut out by an irreducible homogeneous polynomial $f \in k[w,x,y]$. Given rational functions $\varphi_0, \varphi_1, \varphi_2 \in k(C_f)$ not all zero, with $g(\varphi_0, \varphi_1, \varphi_2) = 0$ for some irreducible homogeneous polynomial $g \in k[r,s,t]$, we get a family of maps

$$C_f(K) \setminus I(K) \to C_g(K)$$
$$p \mapsto [\varphi_0(p) : \varphi_1(p) : \varphi_2(p)]$$

where K any extension field of the base field, and $I(K) \subset C_f(K)$ is the finite subset of points at which some φ_i has a pole or at which all of them vanish. The family of these maps only depends on the point $\varphi = [\varphi_0 : \varphi_1 : \varphi_2] \in \mathbb{P}^2(k(C_f))$. We call φ a *rational map* and write

$$\varphi = [\varphi_0 : \varphi_1 : \varphi_2] : C_f \dashrightarrow C_g$$

and this map is *birational* if it has inverse. We also say φ is *morphism* if it is defined at every point $p \in C_f(K)$, and if φ and its inverse are morphisms beside being birational so φ is called an *isomorphism*.

The significance of the following lemma lies in its ability to transition to what is referred to as the *long Weierstrass form*:

Lemma 3.12. *If $C_f \subset \mathbb{P}^2$ is smooth, then any rational map $\varphi : C_f \dashrightarrow C_g$ is a morphism. Hence any birational map between smooth curves is an isomorphism.*

proof. Given a point p in the smooth curve C_f over an extension field K. We say that a rational map, as we define above, is defined at $p \in C_f(K)$ if it can be written in the form $\varphi = [\psi_0 : \psi_1 : \psi_2]$ where $\psi_i = \dfrac{u}{v}$ and $v(p) \neq 0$ with the smallest order of vanishing. Since the order of vanishing for each ψ greater than or equal zero, it follows that the rational map φ is defined at p. **Note:** we can have a birational map between the curve cut of by the cusp and $\mathbb{P}^2$, but it cannot be extend to a morphism since we loss the condition of the smoothness.

Theorem 3.13. *Let E be an elliptic curve with rational point $\boldsymbol{O} \in E(k)$. Then*

i *There exist an isomorphism $\varphi : E \to C_f \subset \mathbb{P}^2$ onto a smooth plane cubic cut out in affine coordinates by an equation in the long Weierstrass form*

$$f(1,x,y) = y^2 + a_1xy + a_3y - (x^3 + a_2x^2 + a_4x + a_6)$$

with $a_i \in k$ such that the point $\boldsymbol{O}$ sent to $\varphi(\boldsymbol{O}) = [0:0:1]$.

ii *If $char(k) \neq 2, 3$, then we can assume that $a_1 = a_2 = a_3 = 0$ so Weierstrass form become short*

$$y^2 = x^3 + a_4x + a_6$$

Proof

To prove the first part: Consider the space $\mathscr{L}(n(\mathbf{O}))$ for $n \geqslant 1$. If we have $x, y \in k(E)$, using Riemann-Roch theorem, $l((\mathbf{O})) = 1$ as $\mathscr{L}((\mathbf{O}))$ is the space of functions have no pole at $\mathbf{O}$ which is the constant functions. Therefore, $\mathscr{L}((\mathbf{O})) =< 1 >$. Also, $l(2(\mathbf{O})) = 2$ so $< 1, x >$ provide a basis for $\mathscr{L}(2(\mathbf{O}))$ as functions have pole at most of order 2, i.e the $ord_{\mathbf{O}}(x) = 2$ and the constant function. Similarly, the set of functions $\{1, x, y\}$ is the generator of $\mathscr{L}(3(\mathbf{O}))$, and $\{1, x, y, x^2\}$ are the generator of $\mathscr{L}(4(\mathbf{O}))$ and so on. Now, $\mathscr{L}(6(\mathbf{O}))$ generate by the functions $\{1, x, y, x^2, xy, x^3, y^2\}$ but $l(6(\mathbf{O})) = 6$, that means there is a linear dependent relation between the generators, i.e $A_1 + A_2x + A_3y + A_4x^2 + A_5xy + A_6x^3 + A_7y^2 = 0$, in this relation we need the coefficients of y^2 and x^3 not both vanish, because both functions have pole of order 6 and if they cancelled out there will have no pole of order 6, to do so we make change of variables $x \to -A_6A_7x$ and $y \to A_6A_7^2y$ and divide through by $A_6^3A_7^4$ and we get the coefficients of y^2 and x^3 are negative to each other and without loss of generality, in Weierstrass form we take them equal 1 so the relation after rescaling becomes

$$f(x,y) = y^2 + a_1xy + a_3y - (x^3 + a_2x^2 + a_4x + a_6) \in k[x,y]$$

for $a_i \in k$ so now we have a rational map $\varphi : E \dashrightarrow C_f$ regarding the previous lemma the map will be an isomorphism if we can show that the curve C_f is smooth. We have $\varphi(\mathbf{O}) = [0:0:1]$ a smooth point and other points in $C_f(\overline{k})$ have the form $p = [1 : x_0 : y_0]$ with $x_0, y_0 \in k$ and then after the translation

$(x, y) \mapsto (x - x_0, y - y_0)$ the polynomial $f(x, y)$ will change, but the new one will still have a long Weierstrass form. Suppose $x_0 = y_0 = 0$ and $[1 : 0 : 0] \in C_f(k)$ is singular point, then the linear terms must vanish so we have a new form $f(x, y) = y^2 + a_1xy - x^3 + a_2x^2$ so the curve is node or cusp, hence we can get a birational map between the curves but we cannot extend it to a morphism and so no isomorphism. This contradiction shows that all the points are smooth and so the curve must be smooth. For second part of the theorem: as the elliptic can define over the extensions fields, we look at the characteristic of the base field. If it has odd characteristic then completing the square via $y \mapsto y - \frac{1}{2}(a_1x + a_3)$ will help to get rid of the terms $a_1xy + a_3y$ and we can make $a_1 = a_3 = 0$ in the reminder terms. If also the characteristic of the base field is not 3, then completing the cube using the substitution $x \mapsto x - \frac{1}{3}a_2$ will get rid the term a_2x^2 and we can make $a_2 = 0$, so we get the short form of Weierstrass equation.

The next proposition constructs a group law of the elliptic using divisors in the Picard group. This approach makes it easier to prove both the associativity and commutativity.

Problema 3.14. Let $(E, \mathbf{O})$ be an elliptic curve over k. Then we have a natural isomorphism of groups

$$\kappa : E(k) \longrightarrow Pic^0(E), P \mapsto ((P) - (\mathbf{O}))$$

proof: Let $P, Q \in E$. It suffices to show $\kappa(P + Q) = \kappa(P) + \kappa(Q)$, The first addition is on E and the second one is addition of divisor classes in $Pic^0(E)$. Let $f(w, x, y) = 0$ gives the line $l \in \mathbb{P}^2$ through P and Q, and let R be the third point of intersection of l with E. Now let $g(w, x, y) = 0$ gives the line $l' \in \mathbb{P}^2$ through R and $\mathbf{O}$, so from the fact that the line $w = 0$ intersects E at $\mathbf{O}$ with multiplicity 3 we can compute the divisor of rational functions

$$div(f/w) = (P) + (Q) + (R) - 3(\mathbf{O})$$

and

$$div(g/w) = (P + Q) + (R) - 2(\mathbf{O})$$

Hence, $div(f/g) = (P + Q) - (P) - (Q) + (\mathbf{O})$ adding and subtraction $\mathbf{O}$ this yield

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

This proves that κ is a group homomorphism.

3.3. The discriminant and j-invariant. Over an algebraically closed field, two elliptic curves are isomorphic if and only if they have the same j-invariant, an important theorem in this section will classify elliptic curves up to isomorphisms.

Lemma 3.15. *Let $E, E' \in \mathbb{P}^2$ be elliptic curves defined by two equations in long Weierstrass form,with the point $\boldsymbol{O}$. Then any isomorphism $\varphi : (E, \boldsymbol{O}) \to (E', \boldsymbol{O})$ is given in affine charts by a coordinate change*

$$(x, y) \mapsto (\lambda^2x + a, \lambda^3y + b\lambda^2x + c)$$

with $\lambda \in k^*$ and $a, b, c \in k$

proof: Let $x, y \in k(E)$ and $x', y' \in k(E')$ be a rational functions on the elliptic curves. The isomorphisms between smooth curves preserve the order of poles and zeros of the rational functions, hence as we prove in 3.13 x' has pole at $\mathbf{O}$ of order 2 and y' has pole at $\mathbf{O}$ of order 3. Therefore, the space $\mathscr{L}(2(\mathbf{O}))$ over E' generated by $< 1, x >$ and $\mathscr{L}(3(\mathbf{O}))$ generated by $< 1, x, y >$ and so

$$\begin{cases} \varphi(x') = \alpha x + a, \\ \varphi(y') = \beta x + \gamma y + c, \end{cases}$$

where $\alpha, \beta \in k^*$ and $\gamma, a, c \in k$. Now (x, y) and (x', y') satisfy Weierstrass equations in form $y^2 + a_1xy + a_3y - (x^3 + a_2x^2 + a_4x + a_6)$ where the coefficients of y^2 and x^3 should be 1, but in case the rational functions x' and y' we will get long Weierstrass equation with λ^2 as coefficient of y^2 and α^3 as coefficient of x^3, then these equations imply $\lambda^2 = \alpha^3$ therefore,

$$\begin{cases} \gamma = \frac{\gamma^3}{\gamma^2} = \frac{\gamma^3}{\alpha^3} = (\frac{\gamma}{\alpha})^3 = \lambda^3, \\ \alpha = \frac{\alpha^3}{\alpha^2} = \frac{\gamma^2}{\alpha^2} = (\frac{\gamma}{\alpha})^2 = \lambda^2 \end{cases}$$

So now E and E' are related by a linear change of variables of the form

$$(x, y) \mapsto (\lambda^2 x + a, \lambda^3 y + b\lambda^2 x + c), b = \lambda^{-2}\beta.$$

However, some different in change of variables in case of short Weierstrass equation:

Corollary 3.16. *Let $E : f(1, x, y) = y^2 - (x^3 - a_4x - a_6)$ and $E' : g(1, x, y) = y^2 - (x^3 - b_4x - b_6)$ with $\boldsymbol{O}$ be elliptic curves defined by short Weierstrass form. If the $char(k) \neq 2, 3$, then any isomorphism $\varphi : (E, \boldsymbol{O}) \to (E', \boldsymbol{O})$ has change of variables of the form $(x, y) \mapsto (\lambda^2 x, \lambda^3 y$ with $a_4 = \lambda^4 b_4$ and $a_6 = \lambda^6 b_6$*

As we have seen in 3.13 any elliptic curve is isomorphic to an elliptic curve cut out by a short Weierstrass equation. Under the assumption that $char(k) \neq 2, 3$ we have

$$f(1, x, y) = y^2 - (x^3 + a_4x + a_6) = 0$$

and we define the *discriminant* and the *j-invariant*, respectively by

$$\triangle(f) = -16(4a_4^3 + 27a_6^2)$$

,

$$j(f) = 1728\frac{4a_4^3}{4a_4^3 + 27a_6^2}$$

Lemma 3.17. *We say the elliptic curve $f : y^2 - x^3 + a_4x + a_6$ smooth if and only if its discriminant is not zero $\triangle(f) \neq 0$*

And this is clear since the polynomial f has a repeated root if and only if it has a root in common with its derivative, so the curve is not smooth and hence the discriminant vanishes.

Theorem 3.18.

- *Two elliptic curves defined over k are isomorphic over $\overline{k}$ if and only if their j-invariant is the same.*
- *If $char(k) \neq 2, 3$, we have $E : y^2 = x^3 + a_4x + a_6$ the automorphism groups of elliptic curves over $\overline{k}$ are given by*

$$Aut_k(E,) \simeq \begin{cases} \mathbb{Z}/4\mathbb{Z}, j(E) = 0, \\ \mathbb{Z}/6\mathbb{Z}, j(E) = 12^3, \\ \mathbb{Z}/2\mathbb{Z}, otherwise \end{cases}$$

3.4. Explict Formula for group operation. In 2 we explained the idea of the group law geometrically for the cubic curve, now we give an explicit formula to compute the addition operation in the elliptic curve in more detail. Suppose we have P_1 and P_2 points on an elliptic curve given by the equation $y^2 = x^3 + Ax + B$ and we want to compute $P_1 + P_2$, draw a line through $P1$ and $P2$ and it will intersect the curve in a third point $P_1 * P_2$, reflect this point across the x-axis will change the sign of the y-coordinate to obtain $P_1 + P_2$, i.e Figure 3.4 make it clear.

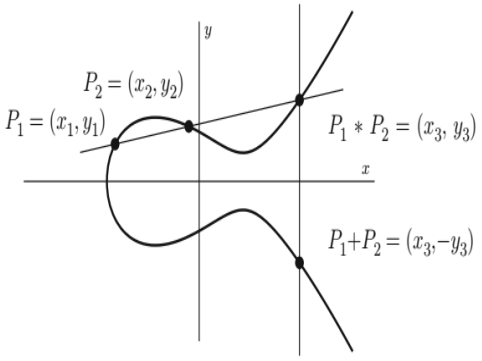

FIGURE 2. Group law: adding two different points in the elliptic curve

- Let
$$P_1 = (x_1, y_1), P_2 = (x_2, y_2), P_1 * P_2 = (x_3, y_3), P_1 + P_2 = (x_3, y_3)$$
The equation of the line through $P1$ and $P2$ is $y = \lambda(x - x_1) + y_1$ with slope given by $\lambda = \dfrac{y_2 - y_1}{x_2 - x_1}$. The intersection with the curve comes from the substitute in the curve's equation to get
$$(\lambda(x - x_1) + y_1)^2 = x^3 + Ax + B$$
Putting everything in one side yield
$$0 = x^3 - \lambda^2 x^2 + \dots$$
The three roots x_1, x_2, x_3 of this cubic correspond to the x-coordinate of the three points of intersection the line with the curve and we knew two from them already, namely x_1 and x_2. Using simple algebra, we could factor a cubic polynomial in form $x^3 + ax^2 + bx + c$ to obtain x_3, the x-coordinate of the third intersection point, and then equating the coefficients as follow
$$x^3 + ax^2 + bx + c = (x - x_1)(x - x_2)(x - x_3) = x^3 - (x_1 + x_2 + x_3)x^2 + \dots$$
Therefore, $x_1 + x_2 + x_3 = -a$, but in our equation $a = \lambda^2$ so the x-coordinate to the third root is
$$x_3 = \lambda^2 - x_1 - x_2$$
Substituting this value in $y = \lambda(x - x_1) + y_1$ we get the $y_3 = \lambda(x_1 - x_3) - y_1$.

- Now consider the case $P_1 = P_2 = (x_1, x_2)$ we can not define the slope as before as the line through the coincide points is a tangent line. Therefore, Implicit differentiation to the curve equation allows us to find the slope
$$2y\frac{dy}{dx} = 3x^2 + A, \lambda = \frac{dy}{dx} = \frac{3x_1^2 + A}{2y_1}$$
Assume $y_1 \neq 0$ so the line equation is $y = \lambda(x - x_1) + y_1$ and we can recover x_3 and y_3 as before but we this time we know only one root, namely x_1 , but it is a double root since the line is tangent at P_1 so we will get
$$x_3 = \lambda^2 - 2x_1, y_3 = \lambda(x_1 - x_3) - y_1.$$
The case where $x_1 = x_2$ but $y_1 \neq y_2$, the line through P_1 and P_2 is a vertical, which therefore intersects the curve in infinity and P_2 is the inverse of P_1 and hence $P_1 + P_2 = \mathbf{O}$.

- If $P_1 = P_2$ and $y_1 = 0$ then $P_1 + P_2 = \mathbf{O}$
- If we add P_1 to $\mathbf{O}$ the line through them is vertical and reflecting point of the intersection will be the point P_1 itself. Hence, $P_1 + \mathbf{O} = P_1$ so $\mathbf{O}$ serves as identity of the group.

4. Application: Primality Testing

Elliptic curves have many applications and uses in many diverse areas of current research in mathematics. However, in this project we present a simple application in number theory, the *test of primalty*, using an elliptic curve over finite field. The primality testing is a version of the classical method called "Pocklington-Lehmer" primality test, it is very important in the field of number theory and plays a huge role in some cryptographic algorithms. In 1986, Goldwasser and Kilian presented the following concept

Theorem 4.1. *Let $n > 1$ and let E be an elliptic curve mod n. Suppose there exist distinct prime numbers $l_1, l_2, \dots, l_k$ and finite points $P_i \in E(\mathbb{Z}_\aleph)$ such that*

- *$l_i P_i = \infty$ for $1 \leqslant i \leqslant k$.*
- *$\prod_{i=1}^{k} l_i > (n^{1/4} + 1)^2$.*

Then n is prime.

Proof
Let p be a prime factor of n. Write $n = p^f n_1$ with $p \nmid n_1$. Then
$$E(\mathbb{Z}_\aleph) = E(\mathbb{Z}_{\beth}) \oplus E(\mathbb{Z}_{\aleph_{\aleph}})$$
Since P_i is a finite point in $E(\mathbb{Z}_\aleph)$, it yields a finite point in $E(\mathbb{Z}_{\beth})$ ($P_i \bmod p^f$). We can further reduce and obtain a finite point $P_{i,p} = P_i \bmod p$ in $E(\mathbb{F}_{\beth})$. Since $l_i P_i = \infty \bmod n$ we have $l_i P_i = \infty$ modulo every factor

of n. In particular, $l_iP_i = \infty$ in $E(\mathbb{F}_l)$, which means that $P_{i,p}$ also has order l_i. It follows that $l_i \mid \sharp E(\mathbb{F}_l)$ for all i, so $\sharp E(\mathbb{F}_l)$ is divisible by $\prod_{i=1}^{k} l_i$. Therefore

$$(n^{1/4}+1)^2 < \prod_{i=1}^{k} l_i < \sharp E(\mathbb{F}_l) < p+1+2\sqrt{p} = (p^{1/2}+1)^2,$$

so $p > \sqrt{n}$. Since all prime factors of n are greater than $\sqrt{n}$, it follows that n is prime.

The idea behind the test is that, choosing a suitable elliptic curve over finite field with appropriate number of points and compute their order, the main advantage here is the vast number of possible elliptic curves that can be used allowing to change if one curve becomes problematic. Although this step could be challenging, many algorithms are efficient in computing the points on elliptic curves, for instance the improved version of "Schoof's algorithm" for Atkin-Elkies. keep searching until an order satisfies

Example 4.2. For $n = 907$. Let $E : y^2 = x^3 + 10x - 2 \bmod n$, and let $l = 71$ then $l > (907^{1/4}+1)^2 \simeq 42.1$
$l = 71$ is the order of $P = (819, 784)$, i.e, $71P = \infty$. Then 907 is prime.
We can repeat the process for l by choosing a appropriate elliptic curve modulo l, and find a point with order satisfy the theorem.

References

[kramer] Krämer Thomas, *Lectures on Elliptic Curves*
[DM] Rosen, Kenneth H, Discrete mathematics and its applications, The McGraw Hill Companies, 2007.
[joseph] Joseph H. Silverman, *The arithmetic of elliptic curves*, Cassels, JWS. **1987**.

Departamento de Matemtica, Universidad Tcnica Federico Santa Mara, Valparaso, Chile.