Elliptic Curves

From curves of genus one to the p-Riemann Hypothesis

Group 18
Jiayi Chen, Irene Hong, Daniel Lin
Zichuan Wang, Baikuan Ye, Yourong Zang[*]

July 18, 2022

Abstract

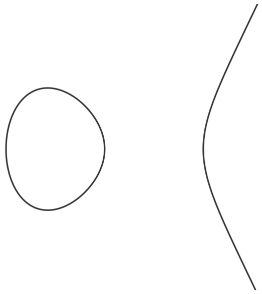
Elliptic curves are smooth curves of genus one with a fixed rational point. From a relatively elementary point of view, they are defined by Weierstrass equations. The group law on elliptic curves can be constructed in two distinct ways, either geometrically or abstractly. We provided a detailed proof of the Mordell's theorem, and some in-depth discussion of elliptic curves in cryptography. This report also includes an introductory exposition to the background and use of Riemann-Roch on elliptic curves. With the help of this powerful algebraic geometry machine, the group was able to construct isogenies and Tate modules on elliptic curves and studied their properties. After obtaining the rejoiceful facts about elliptic curves and the endomorphisms on them, we would prove the Hasse bound and Weil conjectures for elliptic curves, from which we obtain the main result of this project — the p-Riemann Hypothesis.

[*] In alphabetical order. Notes on contributions by sections: 1 — Daniel Lin; 2 — Daniel Lin; 3 — Irene Hong, Daniel Lin and Baikuan Ye; 4 — Jiayi Chen and Zichuan Wang; 5 — Yourong Zang; 6 — Yourong Zang; 7 — Yourong Zang; 8 — Baikuan Ye and Daniel Lin; 9 — Yourong Zang.

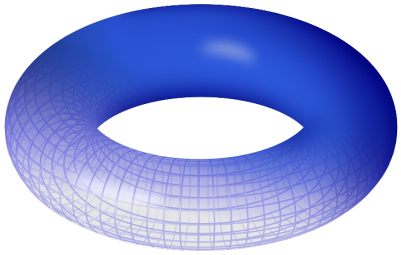
Contents

0 Introduction

The theory of elliptic curves is a major part of modern number theory. Elliptic curves, which are curves defined by Weierstrass equations or smooth curves of genus one (see Theorem 6.1.1 for the equivalence), are fundamental objects with superb properties and applications.



(a) The elliptic curve $E : y^2 = x^3 - x$



(b) An elliptic curve over $\mathbb{C}$ from [Wik22]

In this report, we will first present a series of elementary results on elliptic curves themselves, elliptic curves over $\mathbb{Q}$ and Mordell's theorem concerning the subgroup $E(\mathbb{Q})$ in some elliptic curve E, and some results about elliptic curves over finite fields. Taking a step further, we will define various abstract geometric tools, applying them to elliptic curves over arbitrary fields. This allows us to see why elliptic curves are so useful — they actually describe a huge family of curves; we could also endow each elliptic curve with an extremely neat abelian structure, algebraically, by creating a map between an elliptic E and the degree-0 part of its Picard group $\operatorname{Pic}^0(E)$. Then, the report will present some essential constructions on elliptic curves, including isogenies, Tate modules and Weil parings.

Now let's consider the Riemann ζ functions, where $\operatorname{Re} s > 1$,

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = \frac{1}{1^s} + \frac{1}{2^s} + \frac{1}{3^s} + \cdots$$

Euler proved that

$$\zeta(s) = \prod_{p \text{ prime}} \frac{1}{1 - p^{-s}}$$

It is possible to define an analytic continuation of ζ denoted by ζ^* which satisfies the functional equation

$$\zeta^*(s) = \zeta^*(1 - s)$$

The prominent Riemann Hypothesis states that if $\zeta(s) = 0$ then $\mathrm{Re}(s) = 1/2$ for nontrivial s. The Riemann zeta function can be generalized to all number fields, summing over the prime ideals of a number field. The fact that there is very close analogy between curves over a finite field and algebraic number fields motivated Emil Artin to define a zeta function of curves over finite fields. Weil and Hasse used the function ζ_C as a tool proving the following bound

$$|N_m - 1 - q^m| \leq 2gq^{\frac{m}{2}}$$

where g denotes the genus of the curve $C/\mathbb{F}_q$ and N_m the number of $\mathbb{F}_{q^m}$-rational points on C. This is known as the Hasse bound.

Weil subsequently made several conjectures about Artin's zeta function generalized to all projective varieties.

$$Z(V/\mathbb{F}_q; T) = \exp\left(\sum_{r=1}^{\infty} \frac{\#V(\mathbb{F}_{q^r})}{r} T^r\right)$$

He conjectured that the zeta function (1) is a rational function, (2) satisfies a functional equation and (3) a version of Riemann Hypothesis called the p-Riemann Hypothesis holds on this zeta function.

The report will follow Hasse's proof of these statements, which is the key motivation that Weil made his conjectures, proving the results for elliptic curves over finite fields. This important result gave rise to many modern theories of geometry and number theory.

Coming back from pure abstraction to practical applications, we introduce the interaction of elliptic curves and cryptography. Working with elliptic curves on finite fields seems no longer geometric, but it allows us to use elliptic curves as an effective object in cryptography. The cryptosystems in the earlier years often encrypt things using functions on the finite field $\mathbb{Z}/p\mathbb{Z}$, which is rather small. But with the help of elliptic curves, one can use the rational points $E(\mathbb{F}_p)$ instead and can work with a larger domain where we can choose the encryption functions.

1 Basic Algebra

1.1 Fields and Galois extensions

Definition 1.1.1. A *field* K is a commutative ring where every nonzero element is a unit. Suppose L is a larger field containing K, then K is said to be a subfield of L.

Definition 1.1.2. If L is a field and K is a subfield of L, then L is a *field extension* of K, denoted by L/K.

By the definition of fields, every extension L/K is a vector space over K. One can define the *degree of extension* as

$$[L : K] := \dim_K(L),$$

which is the dimension of this vector space over K. For example, $[\mathbb{C} : \mathbb{R}] = 2$, $[\mathbb{R} : \mathbb{Q}] = \infty$. For elements α_i in L, we define $K(\alpha_1, ..., \alpha_n)$ to be the minimal subfield of L that contains K and all α_i. This is simply the fraction fields of the algebra $K[\alpha_1, ..., \alpha_n]$.

Definition 1.1.3. A field extension L/K is said to be *finite* if $[L : K] < \infty$.

Definition 1.1.4. Given field K, an element α (not necessarily in K) of some field extension L/K is *algebraic* over K if α is root of some polynomial $p(x) \in K[x]$. Otherwise, α is called transcendental.

Remark 1.1.1. Clearly all elements of the ground field K is algebraic over K.

Definition 1.1.5. A field extension L/K is called an *algebraic extension* if all elements of L are algebraic over K.

The following lemma is immediate if we write out the set $\{1, \alpha, \alpha^2, \dots\}$ and argue about its linear dependence.

Lemma 1.1.1. *If M/K is a field extension then $\alpha \in M$ algebraic over K if and only if α is contained in a finite extension of K.*

Remark 1.1.2. This, together with Corollary 1.1.1, suggests that α is algebraic if and only if $K(\alpha)/K$ is finite, since it's the smallest field extension of K containing α.

Lemma 1.1.2 (Tower theorem)**.** *For a tower of fields $M/L/K$,*

$$[M : K] = [M : L][L : K]$$

where both sides are either finite or infinite at the same time.

Proof. The case where one extension is infinite is clear, as we have an infinite set of elements linearly independent over K.

Now suppose both L/K and M/L are finite. Choosing a basis for L over K, say $\{a_1, ..., a_r\}$ and a basis of M over L, say $\{b_1, ..., b_s\}$. Then the set of products $b_i a_j$ can be shown to be linearly independent in M and spans M. So the dimension of M over K is just $rs = [M : L][L : K]$. □

Corollary 1.1.1. *For a tower of fields $M/L/K$, L/K and M/L are finite if and only if M/K is finite.*

Corollary 1.1.2. *Given a field extension L/K, if $\alpha, \beta \in L$ are algebraic over K, then $\alpha + \beta, \alpha\beta, \alpha - \beta, \alpha/\beta$ (if $\beta \neq 0$) are all algebraic over K.*

Proof. Note $K(\alpha, \beta)/K(\alpha)/K$ where each extension is finite as α, β are algebraic. Thus, $K(\alpha, \beta)/K$ is finite which contains $\alpha + \beta, \alpha\beta, \alpha - \beta, \alpha/\beta$. □

For an arbitrary polynomial $p(x)$ over field K, one may wonder if there is always a field L where f has a root in L, and if there is a field M in which f splits into linear factors. And one can ask if a smallest such field exists.

Definition 1.1.6. A field M/K is the *splitting field of a polynomial* $p(x) \in K[x]$ if M is the smallest among fields where $p(x)$ splits into linear factors in M.

Remark 1.1.3. If $\alpha_1, \ldots, \alpha_n$ are roots of p in M, then $M = K(\alpha_1, \ldots, \alpha_n)$.

Lemma 1.1.3. *Given a field K and $f \in K[x]$, there is some finite L/K, unique up to isomorphism, where f splits.*

The isomorphisms between splitting fields may not be unique. Splitting fields can be defined on any set of polynomials. When we define it on the whole polynomial ring $K[X]$, we get an algebraic closure.

Definition 1.1.7. An field L is *algebraically closed* if all polynomials in $L[x]$ have roots in L.

Definition 1.1.8. Given a field K, an algebraic extension L/K is called an *algebraic closure* of K if it is algebraically closed.

Algebraic closures are unique up to isomorphisms. Therefore, in the following section we denote the ground field by k and its algebraic closure by K.

Using Zorn's lemma we obtain

Theorem 1.1.1. *Any field k has an algebraic closure.*

In an algebraic extension, we have the following theorem:

Theorem 1.1.2. *The following statements are equivalent for an algebraic extension L/k*

(i) *Any polynomial $p \in k[x]$ that is irreducible and has a factor in L factors into linear factors in $L[x]$. i.e. if any one root is in L, then all other roots are in L.*

(ii) *L is the splitting field of some set of polynomials over k.*

(iii) *Extend L to algebraic closure K/k containing L. Any automorphism of K that fixes all elements of k maps L to L.*

If an algebraic extension L/k satisfies any of the statements above, it is said to be a normal extension of k

Lemma 1.1.4. *Any algebraic extension L/k of index 2 is normal.*

Proof. Since $[L : k] = 2$, $L = k(\alpha)$ for some α, and $\alpha^2 + b\alpha + c = 0$ for some $b, c \in k$. If β is another root of this polynomial, we have $\beta + \alpha = -b$, meaning $\beta = -b - \alpha \in L$. So the extension is normal. □

Example 1.1.1. One may wish that if $M/L, L/k$ are normal, then M/k is normal. But consider $k = \mathbb{Q}$, $L = \mathbb{Q}(\sqrt{2})$, $M = \mathbb{Q}(\sqrt[4]{2})$, each extension L/k, M/L has degree 2 so they must be normal. But the polynomial $x^4 - 2 \in k[x]$ has roots $\pm\sqrt[4]{2}$ and $\pm\sqrt[4]{2}i$. The last two roots are complex, so they cannot be in M, meaning M/k is not normal.

Definition 1.1.9. A polynomial $p(x) \in k[x]$ is *separable* if it factors over the algebraic closure K as $\prod(x - \alpha_i)$ where α_i are all distinct. i.e. there is no repeated root. This is equivalent to $\gcd(p, p') = 1$ in $k[x]$.

Definition 1.1.10. Given field extension L/k, an element $\alpha \in L$ is *separable* over k if it is root of a separable polynomial in $k[x]$. If all elements of L is separable, L/k is a *separable extension.*

So for L/k, given an irreducible polynomial $f \in k[x]$ of degree n with $\alpha \in L$ being one of its roots, if $k \subseteq L$ is normal, then f has n roots in L; if further L/k is separable, f has n distinct roots in L.

Lemma 1.1.5. *All finite field extensions $\mathbb{F}_{p^m}/\mathbb{F}_{p^n}$ (where $m \geqslant n$) are separable*

Proof. Recall all elements of $\mathbb{F}_{p^m}$ are roots of $f = x^{p^m} - x$. Since $p^n \mid p^n$, $f' = -1$ and $\gcd(f, f') = 1$, meaning f is separable. So this extension is separable. □

Definition 1.1.11. A field extension L/k is *purely inseparable* if any $\alpha \in L$ is a root of $x^{p^n} - a$ for some $a \in k$. Over K, this polynomial equals $(x - \sqrt[p^n]{a})^{p^n}$, which is far from having distinct roots.

Theorem 1.1.3. *For any field extension L/k, there is a field k^{sep} s.t. k^{sep}/k is separable extension and L/k^{sep} is purely inseparable extension.*

In fact, k^{sep} is just the field consisting of all separable elements of L. Now we define *Galois extensions* in several equivalent ways

Theorem 1.1.4. *The following are equivalent for the extension (not necessarily finite) M/k and* the Galois group $G = \text{Gal}(M/k) = \{\sigma \in \text{Aut}(M) : \forall x \in k, \sigma(x) = x\}$

(i) *The extension is algebraic, normal and separable.*

(ii) *The* fixed field $M^G = \{x \in M : \forall \sigma \in G, \sigma(x) = x\}$ *(which is a subfield of M) is k.*

The Galois group of some fields are easier:

Definition 1.1.12. A field k is *perfect* if one of following equivalent conditions holds:

(i) Every irreducible polynomial over k is separable.

(ii) Every algebraic extension of k is separable.

Therefore, if k is a perfect field, the Galois group $\text{Gal}(K/k)$ only fixes k where K is an algebraic closure of k (thus algebraic and normal; and K is separable as k is perfect).

1.2 Miscellaneous

Lemma 1.2.1. *Suppose A is an abelian group and $d : A \to \mathbb{Z}$ a positive definite quadratic form. Then*

$$|d(a-b) - d(a) - d(b)| \leqslant 2\sqrt{d(a)d(b)}$$

for all $a, b \in A$.

Proof. If $a = 0$ then we are done. Suppose $a \neq 0$. Let $L(a,b) = d(a,b) - d(a) - d(b)$ which is a $\mathbb{Z}$-bilinear form. Then since d is positive definite, for all $m, n \in \mathbb{Z}$,

$$0 \leqslant d(ma - nb) = m^2 d(a) + mnL(a,b) + n^2 d(b)$$

Let $m = -L(a,b)$ and $n = 2d(a)$. We obtain

$$d(a)\left(4d(a)d(b) - L(a,b)\right) \geqslant 0$$

which gives the result as $a \neq 0$. □

2 Basic Algebraic Geometry

2.1 Affine varieties

Given an algebraically closed field K, we define the affine n-space to be

$$\mathbb{A}^n(K) = \{(x_1, \cdots, x_n) : x_i \in K\}$$

namely the set of n-tuples of elements of K. When the field used is clear, $\mathbb{A}^n$ is used instead. For any polynomial $f \in K[X_1, \cdots, X_n]$, it naturally defines a map $f : \mathbb{A}^n \to K$ by $(x_1, \cdots, x_n) \mapsto f(x_1, \cdots x_n)$. This f is usually called a *polynomial function.*

Definition 2.1.1. Given set of polynomials $S \subset K[X_1, \cdots, X_n]$, an *an affine algebraic set* is a set of the form

$$\mathbb{V}(S) = \{x \in \mathbb{A}^n : f(x) = 0, \forall f \in S\}$$

if $S = \{f_1, \ldots, f_n\}$, we write $\mathbb{V}(f_1, \ldots, f_n)$ instead. We call a set $X \subseteq \mathbb{A}^n$ *algebraic* if $X = \mathbb{V}(S)$ for some set S.

Some basic algebraic geometry results:

Theorem 2.1.1. (i) $\mathbb{V}(0) = \mathbb{A}^n$. *If K is infinite,* $\mathbb{V}(K[X_1, \cdots, X_n]) = \emptyset$.

(ii) *If $I = (S)$ (the ideal generated by S),* $\mathbb{V}(S) = \mathbb{V}(I)$

(iii) *If $\{I_\alpha\}$ is a collection of ideals,* $\mathbb{V}(\bigcup_\alpha I_\alpha) = \bigcap_\alpha \mathbb{V}(I_\alpha)$.

(iv) *If $I \subseteq J$, then* $\mathbb{V}(I) \supseteq \mathbb{V}(J)$

(v) *For ideals I_1, I_2,* $\mathbb{V}(I_1 \cap I_2) = \mathbb{V}(I_1) \cup \mathbb{V}(I_2)$.

Definition 2.1.2. Given subset $X \subseteq \mathbb{A}^n$, the *ideal of* X is

$$\mathbb{I}(X) = \{F \in K[X_1, \cdots X_n] : F(a_1, \cdots, a_n) = 0, \forall (a_1, \cdots, a_n) \in X\}$$

Definition 2.1.3. If $V = V_1 \cup V_2$, for some proper subsets V_1, V_2 of V, then V is called *reducible.* Otherwise V is called *irreducible.* An irreducible algebraic set is an *affine variety.*

Lemma 2.1.1. *V is irreducible if and only if $\mathbb{I}(V)$ is prime.*

Definition 2.1.4. The *coordinate ring* of a subset V of $\mathbb{P}^n$ is the quotient

$$K[V] = K[x_1, \ldots, x_n]/\mathbb{I}(V)$$

which is an integral domain if V is an (affine) variety.

Define the *Zariski Topology* on $\mathbb{A}^n$ by taking the algebraic sets as closed sets. It is indeed a topology by the key properties of algebraic sets. The Zariski topology on $\mathbb{A}^n$ induces a topology on any subset $W \subset \mathbb{A}^n$ by defining it to be the subspace topology on W. If V is irreducible (i.e. V is variety), W is a *subvariety* of V if it is an irreducible closed subset of V.

2.2 Projective varieties

In order for any two lines in affine space to have intersection, even parallel ones, we need the following definition

Definition 2.2.1. The *projective n-space over K* $\mathbb{P}^n = \mathbb{P}^n(K)$ is the set of all lines through origin in $\mathbb{A}^{n+1}$. Equivalently, $\mathbb{P}^n$ is set of equivalence classes on $\mathbb{A}^{n+1} \setminus \{0\}$ under equivalence relation

$$(x_0, \cdots, x_n) \sim (y_0, \cdots, y_n) \text{ if and only if } \exists \lambda \in K^*, y_i = \lambda x_i, \forall i$$

The equivalence class of $(x_0, \cdots, x_n)$ is denoted by $[x_0 : \cdots : x_n]$.

Given a homogeneous polynomial $F \in K[x_0, \cdots, x_n], P \in \mathbb{P}^n$, $F(P) = 0$ means $F(x_0, \cdots, x_n) = 0$ for any choice of Representatives of P. With this definition, we can move the definition of algebraic sets to the projective space (called *an projective algebraic set in* $\mathbb{P}^n$) $\mathbb{V}(S) = \{P \in \mathbb{P}^n : F(P) = 0, \forall F \in S\}$ where S is a set of homogeneous polynomial in $K[x_0, \ldots, x_n]$. An irreducible projective algebraic set is called a *projective variety* (subvariety defined in the same way). The Zariski topology can also be defined on $\mathbb{P}^n$ by taking projective algebraic sets as closed sets.

3 Elliptic Curves

One might be surprised that the origin of elliptic curves, one of the most essential objects of modern number theory, came out of the study of calculus — the study of elliptic integrals, where they got their names [SS97]. After years of study, people realized that smooth curves of genus one with a rational point can be classified easily with a simple form of equations.

3.1 Weierstrass normal forms

Recall that we have a perfect field k and its algebraic closure K, and we will continue to use these notations in the rest of the report. In this section we assume that $\operatorname{char} k \neq 2, 3$, A cubic is the zero locus of some homogeneous polynomial $f(x, y, z)$ of degree 3 in $\mathbb{P}^2$. Any cubic C (possibly singular) can be transformed into a specific form known as the *Weierstrass normal form*. Note the proof here is a bit sketchy, since there is a detailed construction of the Weierstrass equation for curves of genus one in Theorem 6.1.1.

We choose a coordinate for the projective plane as follow:

(1) Fix a k-rational point $\mathcal{O}$ on a cubic C. Define $Z = 0$ to be the tangent line of C at $\mathcal{O}$.

(2) Define $X = 0$ to be the tangent line of C at the third intersection of $Z = 0$ and the cubic.

(3) Define $Y = 0$ to be any line going through $\mathcal{O}$ other than $Z = 0$.

Dehomogenizing, we get the equation

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

Some linear transformations (with the assumption that $\operatorname{char} k \neq 2, 3$) yield the *Weierstrass normal form of C*

$$y^2 = x^3 + ax^2 + bx + c.$$

If the roots of the RHS are distinct, the cubic curve C is called an *elliptic curve*. Homogenizing this form, we have

$$Y^2Z = X^3 + aX^2Z + bXZ^2 + cZ^3$$

which intersection with the line $Z = 0$ is $X^3 = 0$, with a triple root at $[0 : 1 : 0]$. So we have a unique point at infinity, which is non-singular. The group law of cubics in Weierstrass normal forms is usually built on this fixed base point. Due to the presence of y^2 on one side, any vertical line only meets the cubic in affine plane at two points, so the third point of intersection must be $\mathcal{O}$.

We are mostly interested in the cases where $a, b, c \in k$ in the Weierstrass normal form of a elliptic curve E (which is equivalent to saying that E/k defined earlier).

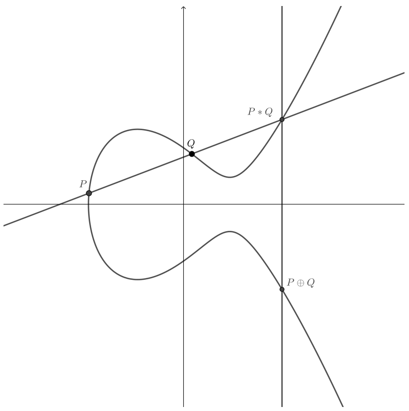
3.2 The geometric group law

In mid-1900s, Weierstrass already made several geometric observations linking the addition of elliptic functions to the addition of points on elliptic curves [Con16]. In 1896, Juel presented the formulas for adding points on elliptic curves, and explicitly described elliptic curves as groups [Jue96].

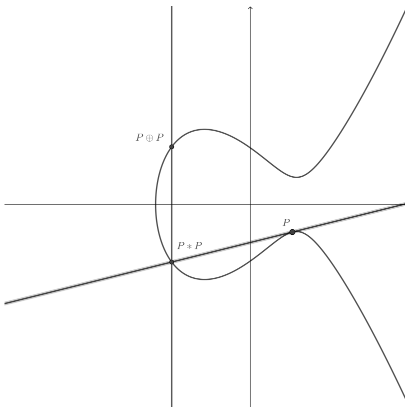
There are two possible (and equivalent) definitions/constructions that endow an elliptic curve with an abelian structure, and we aim to include both in this report. As before, an easier and geometric but hard to prove definition is first presented. The **algebraic construction** and the equivalence of the two constructions are addressed and proved in Section 6.2

By Bézout theorem, the intersection of any line and any elliptic curve consists of three points, counting multiplicities.

Given an elliptic curve E with base point $[0:1:0]$ and two distinct points P, Q on it, we can define a composition $P * Q$ to be the third point of intersection of the line joining P, Q with the cubic. Note that if P, Q are k-rational points, the line passing them is defined over k. If E/k, then the point $P * Q$ is also k-rational as it's described by two equations with rational coefficients. If $P = Q$, then let $P * P$ be the other intersection of the tangent line L at P and E. Unfortunately, there is no identity element for this composition law. Therefore, we fix a rational point $\mathcal{O}$ on E, and define $P \oplus Q$ to be the third intersection of the line joining $P * Q$ and $\mathcal{O}$. Now we have $P \oplus \mathcal{O} = \mathcal{O} \oplus P = P$.



(a) $P \oplus Q$



(b) $P \oplus P$

Theorem 3.2.1. *Suppose E is an elliptic curve and $\oplus$ is the composition law defined above. Then $(E, \oplus)$ is an abelian group. If E/k, then $(E(k), \oplus)$ forms a subgroup.*

The composition law is therefore called the group law on E, and we use $+$ instead of $\oplus$.

Proof. The operation is commutative since the construction of $P * Q$ is symmetric. The existence of an identity is mentioned above. The inverse $-Q$ of Q can be constructed by drawing a tangent line at $\mathcal{O}$, finding the third point of intersection S with E, and finding the third point of intersection of the line joining Q, S and the curve. The associativity is rather hard to prove. One may choose to argue geometrically, or simply writing down the explicit formulas. □

3.3 Explicit formulas for the group law

Let E be an elliptic curve defined by

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

Lemma 3.3.1. *If $P_0 = (x_0, y_0) \in E$, then $-P_0 = (x_0, -y_0 - a_1x_0 - a_3)$.*

Proof. In order to calculate $-P_0$, we take the line L through P_0 and $\mathcal{O}$ and finds its third point of intersection with E. The line L is given by

$$L : x - x_0 = 0.$$

Substituting this into the equation for E, we see that $F(x_0, y)$ has two roots y_0 and y_0', where $-P = (x_0, y_0')$. Writing out

$$F(x_0, y) = c(y - y_0)(y - y_0')$$

and equating the coefficients of y^2 gives $c = 1$, and similarly equating the coefficients of y gives $y_0' = -y_0 - a_1x_0 - a_3$. This yields

$$-P_0 = (x_0, -y_0 - a_1x_0 - a_3).$$

□

Lemma 3.3.2. *Let $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$ be points on E. If $x_1 = x_2$ and $y_1 + y_2 + a_1x_1 + a_3 = 0$, then by Lemma 3.3.1,*

$$P_1 + P_2 = \mathcal{O}.$$

Otherwise define

$$\lambda = \begin{cases} \frac{y_2 - y_1}{x_2 - x_1}, & x_1 \neq x_2 \\ \frac{3x_1^2 + 2a_2x_1 + a_4 - a_1y_1}{2y_1 + a_1x_1 + a_3}, & x_1 = x_2 \end{cases}, \quad \nu = \begin{cases} \frac{y_1x_2 - y_2x_1}{x_2 - x_1}, & x_1 \neq x_2 \\ \frac{-x_1^3 + a_4x_1 + 2a_6 - a_3y_1}{2y_1 + a_1x_1 + a_3}, & x_1 = x_2 \end{cases}$$

Then $y = \lambda x + \nu$ is the line through P_1, P_2 or tangent to E if $P_1 = P_2$.

Proof. The proof of this lemma is trivial — do some elementary computations! □

And we are ready to compute the addition formula of two points:

Lemma 3.3.3. *Let $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$ be points on E, and the equation through P_1 and P_2 (or the tangent line to E if $P_1 = P_2$) be $y = \lambda x + \nu$. Then we have that*

$$P_1 + P_2 = (\lambda^2 + a_1\lambda - a_2 - x_1 - x_2, -(\lambda + a_1)x_3 - \nu - a_3).$$

Proof. Substituting the equation of L into the equation of E, we see that $F(x, \lambda x+\nu)$ has roots x_1, x_2, x_3, where $P_3 = (x_3, y_3)$ is the third point of $L \cap E$. We write out

$$F(x, \lambda x + \nu) = c(x - x_1)(x - x_2)(x - x_3)$$

and equate coefficients. The coefficient of x^3 gives $c = -1$, and then the coefficient of x^2 gives $x_3 = \lambda^2 + a_1\lambda - a_2 - x_1 - x_2$. And substituting x_3 into the equation of L gives the value of $y_3 = \lambda x_3 + \nu$. □

Corollary 3.3.1. *When $P_1 \neq P_2$, we have*

$$x(P_1 + P_2) = \frac{y_2 - y_1}{x_2 - x_1}^{2} + a_1\frac{y_2 - y_1}{x_2 - x_1} - a_2 - x_1 - x_2,$$

and the duplication formula *for $P = (x, y) \in E$,*

$$x([2]P) = \frac{x^4 - b_4x^2 - 2b_6x - b_8}{4x^3 + b_2x^2 + 2b_4x + b_6},$$

where $b_2 = a_1^2$, $b_4 = 2a_4+a_1a_3$, $b_6 = a_3^2+4a_6$, and $b_8 = a_1^2a_6+4a_2a_6-a_1a_3a_4+a_2a_3^2-a_4^2$.

3.4 Important invariants

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

and an extra point $O = [0, 1, 0]$ out at infinity.
If $\mathrm{char}(K) \neq 2$, we can simplify the equation into the form

$$E : y^2 = 4x^3 + b_2x^2 + 2b_4x + b_6,$$

where

$$b_2 = a_1^2 + 4a_4, \qquad b_4 = 2a_4 + a_1a_3, \qquad b_6 = a_3^2 + 4a_6.$$

We also define quantities:

$$b_8 = a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2,$$

$$c_4 = b_2^2 - 24b_4.$$

Definition 3.4.1. The quantity Δ is the discriminant of the Weierstrass equation, defined by

$$\Delta = -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6.$$

The j-invariant of the elliptic curve is given by

$$j = c_4^3/\Delta.$$

Remark 3.4.1. Assuming that the characteristic of K is not 2 or 3, take an elliptic curve and write it in Weierstrass form

$$E : y^2 = x^3 + Ax + B.$$

The discriminant of the Weierstrass equation is then given by

$$\Delta = -16(4A^3 + 27B^2).$$

And the j-invariant of the elliptic curve is given by

$$j = -1728\frac{(4A)^3}{\Delta}.$$

Theorem 3.4.1. *The curve given by a Weierstrass equation satisfies:*

(i) *It is nonsingular if and only if* $\Delta = 0$.

(ii) *It has a node if and only if* $\Delta = 0$ *and* $c_4 \neq 0$.

(iii) *It has a cusp if and only if* $\Delta = c_4 = 0$.

In cases (ii) and (iii), there is only the one singular point.

Theorem 3.4.2. *Two elliptic curves are isomorphic over* K *if and only if they both have the same* j*-invariant.*

Proof. First, if two elliptic curves are isomorphic, then the transformation formulas show that they have the same j-invariant.
For the converse, we will assume that $\text{char}(K) \geq 5$. Let E and E' be the elliptic curves with the same j-invariant with the Weierstrass equations

$$E : y^2 = x^3 + Ax + B,$$

$$E' : y'^2 = x'^3 + A'x' + B'.$$

Then by the assumption $j(E) = j(E')$, we have that

$$\frac{(4A)^3}{4A^3 + 27B^2} = \frac{(4A')^3}{4A'^3 + 27B'^2},$$

which yields

$$A^3B'^2 = A'^3B^2$$

In order to find an isomorphism of the form $(x, y) = (u^2x', u^3y')$, we consider three cases:

(i) $A = 0$ $(j = 0)$. Since $\Delta = -16(4A^3 + 27B^2) \neq 0$, $B \neq 0$, so $A' = 0$. And we obtain an isomorphism using $u = (B/B')^{1/6}$.

(ii) $B = 0$ $(j = 1728)$. Then $A \neq 0$, so $B' = 0$, and we take $u = (A/A')^{1/4}$.

(iii) $AB \neq 0$ $(j \neq 0, 1728)$. If one of A', B' were 0, then both of them would be 0, and Δ' would be 0, which is a contradiction. Therefore, $A'B' \neq 0$, and $u = (A/A')^{1/4} = (B/B')^{1/6}$ gives an isomorphism.

□

Theorem 3.4.3. *Let $j_0 \in K$. There exists an elliptic curve defined over $K(j_0)$ whose j-invariant is equal to j_0.*

For consistency we define the *invariant differential on an elliptic curve E* here: suppose $E; y^2 + a_1y + a_3 = x^2 + a_2x^2 + a_4x + a_6$, then the differential form

$$\omega = \frac{dx}{2y + a_1x + a_3}$$

and we claim, without proof, that the invariant differential is regular and nonvanishing. The relevant terminologies will not be defined and used until Section 5.6

4 Elliptic Curves over $\mathbb{Q}$: Mordell-Weil Theorem

A brief introduction to the study of Elliptic Curves. The study of Elliptic Curves could trace back to ancient Greece, when Diophantus of Alexandria, one of the great ancient mathematicians, formulated and solved many problems about the solution of polynomial equations in either integers or rational numbers, that is, the solution of

$$F(x_1, \cdots, x_n) = 0$$

where F is a polynomial in n variables. The case of the polynomials in one variable is straightforward, as well as linear polynomials in two variables.

The case of quadratic polynomials is solved by Hasse principle, namely:

Theorem 4.0.1 (Hasse principle)**.** *A homogeneous quadratic equation in several variables is solvable by integers, not all zero, if and only if it is solvable in real numbers and in p-adic numbers for each prime p.*

Therefore the next easiest case would involve cubic polynomials in two variables. In this section, we present the Mordell's Theorem, a weaker version of the Mordell-Weil theorem: the group of rational points on a smooth cubic curve is finitely generated. We firstly need to define the height of a rational point on a smooth cubic curve $C : y^2 = x^3 + ax^2 + bx$. To start with, we define the *height* of a rational point on the cubic C.

4.1 Height of points

Definition 4.1.1. Let $x = \frac{m}{n}$ be a rational number in lowest terms. The *height* of x is a positive number that defined to be the maximum of the absolute values of the numerator and the denominator of x.

$$H(x) = H\left(\frac{m}{n}\right) = \max\{|m|, |n|\}.$$

We can see the heights of rational points measure the complexity of rationals in a number-theoretic sense. Now consider an example:

Example 4.1.1. let $a = 1$, $b = \frac{999}{1000}$. These two rational numbers are very close to each other but there is a large difference in their heights.

Definition 4.1.2. Let $P = (x, y)$ be a rational point on the curve C. The *height* of P is the height of its x-coordinate.

$$H(P) = H(x)$$

$H(\mathcal{O})$ is set to be 1. We also define a *"new" height* for rational points on elliptic curve by just taking the logarithm of heights which is more convenient for our further works

$$h(P) = \log H(P)$$

Remark 4.1.1. It is easy to see that the set of all rational numbers whose height is less than some fixed number is a finite set. To see this, take $x = m/n < r$ in lowest terms for some real number r, then both $|m|, |n| < r$. Hence only finitely m and n in this set. Note that the set of all rational points on an elliptic curve also obeys the fact above. Indeed, for each of the possible x-coordinates of height less than r there are at most two distinct y-coordinates for an elliptic curve. As the number of x-coordinates is finite, the number of points in this set is also finite. We conclude the discussion above with the following lemma:

Lemma 4.1.1. *For every real number r, the set $\{P \in C(\mathbb{Q}) : h(P) < r\}$ is finite*

4.2 Bounding the heights

To prove Mordell's Theorem, more lemmas are needed, which we present below:

Lemma 4.2.1. *Let P_0 be a fixed rational point of C. Then there is a constant κ_0 which depends on P_0, a, and b such that*

$$h(P + P_0) \leqslant 2h(P) + \kappa_0$$

for all $P \in C(\mathbb{Q})$.

In order to prove this lemma, we need to assume some results:

Lemma 4.2.2. *Let $P = (x, y)$ be a rational point on C. Then*

(i) *We can write x and y by $x = \frac{m}{d^2}, y = \frac{n}{d^3}$ for some integers m, n, d with $d > 0$ and $\gcd(m, d) = \gcd(n, d) = 1$.*

(ii) *There is some $K > 0$ depending only on a, b, C such that $|m| \leqslant H(P), |d| \leqslant H(P)^{\frac{1}{2}}, |n| \leqslant KH(P)^{\frac{2}{3}}$.*

Proof. Let $P = (x, y), P_0 = (x_0, y_0)$, and $P + P_0 = (x', y')$. Then $H(P + P_0) = H(x')$. Using the results from explicit formulas for the group law we can write $x' + x + x_0 =$

$\lambda^2 - a$ with $\lambda = \frac{y-y_0}{x-x_0}$. Proceed by rearranging

$$\begin{aligned} x' &= \left(\frac{y-y_0}{x-x_0}\right)^2 - a - x - x_0 \\ &= \frac{(y-y_0)^2 - (a+x+x_0)(x-x_0)^2}{(x-x_0)^2} \\ &= \frac{y^2 - 2yy_0 + y_0^2 - (a+x+x_0)(x-x_0)^2}{(x-x_0)^2} \\ &= \frac{x^3 + ax^2 + bx - 2yy_0 + y_0^2 - (a+x+x_0)(x-x_0)^2}{(x-x_0)^2} \\ &= \frac{-2y_0y + x_0x^2 + (b + 2x_0a + x_0^2)x + (y_0^2 + ax_0^2 + x_0^3)}{x^2 - 2xx_0 + x_0^2} \\ &= \frac{Ay + Bx^2 + Cx + D}{Ex^2 + Fx + G} \end{aligned}$$

Where $\{A, B, ..., G\}$ are rational numbers depending on a, b, x_0, y_0. Furthermore, we can multiply the expression by their least common denominator to assume $\{A, B, ..., G\}$ are integers.

By (i) in Lemma 4.2.2, we can write

$$x' = \frac{A\frac{n}{d^3} + B\left(\frac{m}{d^2}\right)^2 + C\frac{m}{d^2} + D}{E\left(\frac{m}{d^2}\right)^2 + F\frac{m}{d^2} + G} = \frac{And + Bm + Cmd^2 + Dd^4}{E + Fm^2 + Gd^4}$$

which means

$$H(x') \leqslant \max\left\{|And + Bm + Cmd^2 + Dd^4|, |E + Fm^2 + Gd^4|\right\}$$

Using (ii) in Lemma 4.2.2, there is some $K > 0$ such that

$$\begin{aligned} \left|And + Bm + Cmd^2 + Dd^4\right| &\leqslant |And| + |Bm| + |Cmd^2| + |Dd^4| \\ &\leqslant (|AK| + |B| + |C| + |D|)H(P)^2 \end{aligned}$$

and

$$\begin{aligned} |E + Fm^2 + Gd^4| &\leqslant |E| + |Fm^2| + |Gd^4| \\ &\leqslant (|E| + |F| + |G|)H(P)^2 \end{aligned}$$

Therefore $H(x') \leqslant \max\{|AK| + |B| + |C| + |D|, |E| + |F| + |G|\}H(P)^2$. Taking the logarithm, we get

$$h(P + P_0) = \log H(x') \leqslant 2h(P) + \kappa_0$$

where $\kappa_0 = \log\max\{|AK| + |B| + |C| + |D|, |E| \ + |F| + |G|\}$ which only depends on a, b, x_0, y_0, completing the proof. □

Remark 4.2.1. The proof above does not apply if $P = P_0, -P_0, \mathcal{O}$. For $P = \mathcal{O}$, the result is trivial, and the other two cases can be avoided using the duplication formula. The inequality still holds because for finitely many P, we can simply look at the differences $h(P + P_0) - 2h(P)$ and take κ_0 larger than the finite number of values that occur.

Lemma 4.2.3. *There is a constant κ, depending on a and b, that*

$$h(2P) \geqslant 4h(P) - \kappa$$

for all $P \in C(\mathbb{Q})$.

We still need some extra results for proving this lemma. Proofs are omitted as they are not especially related to elliptic curves.

Lemma 4.2.4. *let $\phi(X), \psi(X)$ be polynomials with integer coefficients and no common complex roots. Let d be the maximum of the degrees of ϕ and ψ.*

(i) *There is an integer $R \geq 1$, depending on ϕ and ψ, so that for all rational numbers m/n*

$$\gcd\left(n^d\phi\left(\frac{m}{n}\right), n^d\psi\left(\frac{m}{n}\right)\right)$$

divides R

(ii) *There are constants κ_1, κ_2, depending on ϕ and ψ, so that for all for for all rational numbers m/n which are not roots of ψ*

$$dh\left(\frac{m}{n}\right) - \kappa_1 \leqslant h\left(\frac{\phi\left(\frac{m}{n}\right)}{\psi\left(\frac{m}{n}\right)}\right) \leqslant dh\left(\frac{m}{n}\right) + \kappa_2$$

By using the results above, we are now ready to give a proof of Lemma 4.2.3.

Proof. Similar as the case of Lemma 4.2.1,ignoring a finite set of points would not affect the inequality. So it is reasonable to discard the finite many points such $2P = \mathcal{O}$. We will see the reason to exclude these points later.
Now assume $P = (x, y), 2P = (x', y')$. Duplication formula applied here:

$x' + 2x = \lambda^2 - a$ with $\lambda = \frac{f'(x)}{2y}$. Proceed by rearranging. Note $y^2 = f(x) = x^3 + ax^2 + bx$ here. Thus,

$$\begin{aligned} x' &= \left(\frac{f'(x)}{2y}\right)^2 - 2x - a \\ &= \frac{f'(x)^2}{4y^2} - (a + 2x) \\ &= \frac{f'(x)^2 - (4a + 8x)f(x)}{4f(x)} \qquad = \frac{(3x^2 + 2ax + b)^2 - (4a + 8x)(x^3 + ax^2 + bx)}{4(x^3 + ax^2 + bx)} \\ &= \frac{x^4 - 2bx^2 + b^2}{4x^3 + 4ax^2 + 4bx} \end{aligned}$$

where the third equality holds because $f(x) \neq 0$ if and only if $2P \neq \mathcal{O}$. Hence x' is a quotient of two polynomials in x with integer coefficients, due to the fact that $f(x)$ is non-singular from assumption, we know that $f(x)$ and $f'(x)$ have no common complex roots. It follows that the polynomials in the numerator and denominator of x' also have no common roots. Since $h(P) = h(x), h(2P) = h(x')$, it is suffice to show $h(x') \geqslant 4h(x) - \kappa$ for this lemma. As and the maximum degree of the polynomials in the numerator and denominator is 4. This inequality could be derived by Lemma 4.2.4 (ii) as the maximum degree of the polynomials in the numerator and denominator is 4 and $h(x) = h(m/n)$. Together with the fact that the polynomials in the numerator and denominator of x' depend on a, b, finishing the proof.

□

Lemma 4.2.5. *The index*

$$[C(\mathbb{Q}) : 2C(\mathbb{Q})]$$

is finite, where $2C(\mathbb{Q})$ is the set of rational points Q that are equal to $P + P$, where P is a rational point on $C(\mathbb{Q})$.

We give an outline for the proof. For the curve $C : y^2 = x^3 + ax^2 + bx$, define $\bar{a} = -2a, \bar{b} = a^2 - 4b$. This gives a new curve $\bar{C} : y^2 = x^3 - 2ax^2 + (a^2 - 4b)x$.

These two curves are closely related. To see this, define the function $\phi : C \to \bar{C}$:

$$(x, y) \to (\bar{x}, \bar{y}) := (\frac{y^2}{x^2}, y\frac{x^2 - b}{x^2}),$$

one could easily show this new point $(\bar{x}, \bar{y})$ is indeed a rational point on $\bar{C}$. Similarly, define $\bar{\phi} : \bar{C} \to \bar{\bar{C}}$:

$$(\bar{x}, \bar{y}) \to (\bar{\bar{x}}, \bar{\bar{y}}) := (\frac{\bar{y}^2}{\bar{x}^2}, \bar{y}\frac{\bar{x}^2 - b}{\bar{x}^2}),$$

then the composition of functions $\bar{\phi} \circ \phi$, gives exactly the endomorphism $C(\mathbb{Q}) \to C(\mathbb{Q}) : P \to 2P$. In specific, both the index $(C(\mathbb{Q}) : \phi(C(\mathbb{Q})))$ and $(\phi(C(\mathbb{Q})) : \bar{\phi}(C(\mathbb{Q})))$ are finite, so as their composition, the index $(C(\mathbb{Q}) : 2C(\mathbb{Q}))$ is also finite.

We would not give a complete proof of Lemma 4.2.5 for similar reasons as Lemma 4.2.4 and Lemma 4.2.2. You can find detailed information of them in [ST15].

4.3 A proof due to Mordell

Mordell presented a proof in 1922 of his theorem concerning the rational points on a cubic curve [Mor22]. A revised proof in modern languages is reproduced below.

Theorem 4.3.1 (Mordell's Theorem)**.** *Let C be a smooth cubic curve given by some equation*

$$C : y^2 = x^3 + ax^2 + bx$$

where a and b are integers, then the rational points on C form a group $C(\mathbb{Q})$, and $C(\mathbb{Q})$ is finitely generated.

Proof. We start with Lemma 4.2.5 that the index $[C(\mathbb{Q}) : 2C(\mathbb{Q})]$ is finite. We can assume that

$$C(\mathbb{Q}) = \bigsqcup_{k=1}^{n} [Q_k + 2C(\mathbb{Q})]$$

for some rational points $Q_1, \ldots, Q_n$. Thus any point $P_0 \in C(\mathbb{Q})$ could be written in the form

$$P_0 = Q_{n_1} + 2P_1$$

for some rational point P_1. Repeating this process for P_1 and subsequently for each P_i, we obtain

$$P_i = Q_{n_{i+1}} + 2P_{i+1}$$

for all $0 \leqslant i \leqslant m - 1$. Combining these results we get:

$$\begin{aligned} P_0 &= Q_{n_1} + 2P_1 \\ &= Q_{n_1} + 2Q_{n_2} + 4P_2 \\ &= Q_{n_1} + 2Q_{n_2} + 4Q_{n_3} + 8P_3 \\ &= \cdots \\ &= Q_{n_1} + 2Q_{n_2} + 4Q_{n_3} + \cdots + 2^{m-1}Q_{n_m} + 2^m P_m \end{aligned}$$

This pattern can repeat forever if needed. The above formula thus indicates that this specific point P is generated by the representatives $Q_1, \cdots, Q_n$ and P_m, but the problem is that P_m depends on P. However, it would be nice if we could show that there are only finitely many possible P_m, say $P_{m_1}, \cdots, P_{m_s}$, no matter which P we choose, because then every point $P \in C(\mathbb{Q})$ could be written as

$$P = 2^{m_j} P_{m_j} + \Sigma_{i=0}^{m_j} a_i Q_{n_i}$$

for some $P_{m_j} \in \{P_{m_1}, \cdots, P_{m_s}\}$.

Notice that it is sufficient to prove that the heights of $P_{m_1}, \cdots, P_{m_s}$ are bounded by some real number M: there are only finitely positive integers less or equal than M, so there are at most $2M^2$ rational points with height no more than M. In particular, this is a finite set of points.

Following this strategy, we now show that all possible P_m's have their height bounded by a certain real number M, by choosing a sufficiently large m. Applying Lemma 4.2.1 to P_m and $-Q_1, \cdots, -Q_n$, one obtains constants κ_i such that

$$h(P_m - Q_i) \leqslant 2h(P_m) + \kappa_i.$$

Let $\kappa_{\max} = \max(\kappa_i)$. We get

$$h(P_m - Q_i) \leqslant 2h(P_m) + \kappa_{\max}$$

for all i. By Lemma 4.2.3, applied to P_m,

$$4h(P_m) \leqslant h(2P_m) + \kappa = h(P_{m-1} - Q_{n_m}) + \kappa \leqslant 2h(P_{m-1}) + \kappa_{\max} + \kappa$$

In the equation we used $P_{m-1} = Q_{n_m} + 2P_m$.

Dividing both sides by four gives

$$h(P_m) \leqslant \frac{h(P_{m-1})}{2} + \frac{\kappa_{\max} + \kappa}{4} = \frac{3}{4}h(P_{m-1}) + \frac{\kappa_{max} + \kappa - h(P_{m-1})}{4}.$$

Now we set $M = \kappa_{max} + \kappa$, and show that $h(P_m) \leq M$ for a sufficiently large m. If $h(P_{m-1}) \leqslant \kappa_{\max} + \kappa$, then we are done. Otherwise we have $h(P_{m-1}) > \kappa_{\max} + \kappa$, which means

$$h(P_m) \leqslant \frac{3}{4}h(P_{m-1}) + \frac{\kappa_{max} + \kappa - h(P_{m-1})}{4} < \frac{3}{4}h(P_{m-1}).$$

Since $3/4 < 1$, it is guaranteed that $h(P_m) \to 0$ as $m \to \infty$. In particular, for a sufficiently large m, $h(P_m) \leq \kappa_{max} + \kappa = M$.

We thus showed for any $P = 2^m P_m + \Sigma_{i=0}^m a_i Q_{n_i}$, and a sufficiently large m, the height of P_m is no more than M. Together with Lemma 4.1.1, we've shown that there are only finitely many possible P_m's. Thus, any point $P \in C(\mathbb{Q})$ is (finitely) generated by

$$\{Q_1, \cdots, Q_n\} \cup \{\text{finitely many possible } P_m\},$$

completing the proof. □

5 More on Curves

5.1 Curves and rational points

We require all varieties in this report to be irreducible.

Definition 5.1.1. A *curve* is a projective variety of dimension 1.

Therefore, we are only interested in projective varieties and most of the objects will be constructed in them. In order to study the rational solutions of a certain type of equations (that is, on some curves), it is important to base all geometric constructions on some algebraically closed extension of the field we are interested in. Say k is a perfect field and K an algebraic closure of k, we denote by $\mathrm{Gal}(K/k)$ the Galois group of K/k (the fixed field of this group is k as K is an algebraic, separable and normal extension of k). We can define a natural group action of $\mathrm{Gal}(K/k)$ on the projective space $\mathbb{P}^n$ over K by $[x_0 : \cdots : x_n]^\sigma = [x_0^\sigma : \cdots : x_n^\sigma]$ for any σ in the Galois group. We introduce the following notations/definitions.

Definition 5.1.2. The *set of k-rational points* $\mathbb{P}^n(k)$ is the set $\{[x_0 : \cdots : x_n] : \forall i, x_i \in k\}$. Given a projective variety V, the *k-rational points of V* is the set $V(k) = V \cap \mathbb{P}^n(k)$.

Definition 5.1.3. A projective variety V is said to be *defined over k*, written as V/k, if $\mathbb{I}(V)$ can be generated by homogeneous polynomials with rational coefficients (i.e., in $k[x_0, \ldots, x_n]$).

Remark 5.1.1. We can also use Galois-theoretic languages:

$$\mathbb{P}^n(k) = \{P \in \mathbb{P}^n : P^\sigma = P, \forall \sigma \in \mathrm{Gal}(K/k)\},$$

and

$$V(k) = \{P \in V : P^\sigma = P, \forall \sigma \in \mathrm{Gal}(K/k)\}$$

as the fixed field of the Galois group is k.

Since we are working with low dimensional cases, it is convenient to define the function field of a projective variety using an affine chart. For any variety W we define

$$k[W] = k[x_0, \ldots, x_n]/\mathbb{I}(W/k)$$

where $\mathbb{I}(W/k) = \mathbb{I}(W) \cap k[x_0, \ldots, x_n]$.

Definition 5.1.4. Given a projective variety V/k, choose some $U_i = \{x_i \neq 0\} \subseteq \mathbb{P}^n$. Define the *function field of* V, $k(V)$, to be the quotient field of $k[V \cap U_i]$ and the *larger function field of* V to be the quotient field of $K[V \cap U_i]$.

Remark 5.1.2. The choice of the chart does not matter — the resulting fields are isomorphic. The elements in $K(V)$ are of the form f/g where f, g are homogeneous polynomials of the same degree in $n+1$ variables, $g \notin \mathbb{I}(V)$.

For some projective variety V, we can define a group action of $\mathrm{Gal}(K/k)$ on $K[V]$ sending $f = \sum a_I x^I$ to $f^\sigma = \sum \sigma(a_I)x^I$, that is, acting on the coefficients of f. We can further extend this group action to $K(V)$ by defining $(f/g)^\sigma = f^\sigma/g^\sigma$. It is easy to check that the invariant sets in $K[V]$ and $K(V)$ are $k[V]$ and $k(V)$ respectively.

Remark 5.1.3. Since $\mathrm{Gal}(K/k)$ consists of field endomorphisms, we have $(f(P))^\sigma = f^\sigma(P^\sigma)$ for all f and points P.

Suppose V_1, V_2 are two projective varieties. For any rational map $\varphi = [f_0 : \cdots : f_n] : V_1 \to V_2$ where $f_i \in K(V_1)$, we define a group action $\varphi^\sigma = [f_0^\sigma : \cdots : f_n^\sigma]$. And by Remark 5.1.3, we get $(\varphi(P))^\sigma = \varphi^\sigma(P^\sigma)$.

Definition 5.1.5. A rational map $\varphi = [f_0 : \cdots : f_n]$ on V is *defined over* k if there exists some nonzero $\lambda \in K$ such that $\lambda f_i \in k(V)$ for all i. Equivalently, $\varphi^\sigma = \varphi$ for all $\sigma \in \mathrm{Gal}(K/k)$.

Definition 5.1.6. For any projective variety V and a smooth point $P \in V$, the maximal ideal at P is $\mathfrak{m}_P = \{f \in K[V] : f(P) = 0\}$. The *local ring of* V *at* P, denoted by $K[V]_P$ is the localization $K[V]_{\mathfrak{m}_P}$ which is simply the local ring

$$K[V]_P = \{f/g : f, g \in K[V] \text{ and } g(P) \neq 0\}$$

A rational function $f \in K(V)$ is said to be regular at P if $f \in K[V]_P$.

These definitions are equivalent to the mostly seen ones, but it would require some nontrivial arguments to prove the equivalence. See [Har10] for instance. They also allow us to do most of our explicit computations on affine coordinate rings, while using the projective varieties to make certain huge theorems work.

Remark 5.1.4. Since for a projective variety V the closure of $V \cap \mathbb{A}^n$ in $\mathbb{P}^n$ is simply V, we will always use the affine variety to represent V and other objects on V.

5.2 Local rings at smooth points

We reproduce Definition 5.1.1 below.

Definition 5.2.1. A *curve* is a projective variety of dimension 1.

In our report, the term curve refers to **smooth** curves, which are curves with all points smooth. Standard algebraic geometry results show that if P is a smooth point of a projective variety V, then the dimension (over K) of $\mathfrak{m}_P/\mathfrak{m}_P^2$ ([Har10]) equals the dimension of V. Thus, given any curve C, we have $\dim_K \mathfrak{m}_P/\mathfrak{m}_P^2 = 1$, which gives us the following commutative algebra result:

Lemma 5.2.1. *For all points P in the curve C, the local ring $K[C]_P$ is a discrete valuation ring with a valuation defined by*

$$\mathrm{ord}_P(f) = \sup\{d \in \mathbb{N} : f \in \mathfrak{m}_P^d\}$$

which is a map $K[C]_P \to \mathbb{N} \cup \{\infty\}$. Furthermore, each valuation ord_P can be extended to $K(C)$ by $\mathrm{ord}_P(f/g) = \mathrm{ord}_P(f/1) - \mathrm{ord}_P(g/1)$. This map is called the order of f/g at P.

Proof. Prop. 9.2 in [AM94]. □

Remark 5.2.1. The fraction field of a localization of some ring is isomorphic to the fraction field of the original ring. Therefore, $K(C)$ is the fraction field of $K[C]_P$ for any P.

Definition 5.2.2. The *uniformizer for C at P* is some element $t \in K(C)$ such that $\mathrm{ord}_P(t) = 1$.

Remark 5.2.2. There certainly exists a uniformizer: since every discrete valuation ring is a principal ideal domain, $\mathfrak{m}_P = (t)$ for some t, which must be of order one as suggested by commutative algebra results.

If $t \in K(C)$ is of order one, then for any $g \in \mathfrak{m}_P$ (meaning $\mathrm{ord}_P(g) \geqslant 1$), we have

$$\mathrm{ord}_P(g/t) = \mathrm{ord}_P(g) - 1 \geqslant 0$$

so $g/t \in K[C]_P$, meaning there exists some $h \in K[C]_P$ such that $g = th$ and thus $\mathfrak{m}_P = (t)$.

To assist further understandings of this valuation, we present the following example.

Example 5.2.1. Consider the curve $y^2 = x^3 + 2x$ over a field K with characteristic not equal to 2, which is smooth. Let $P = (0,0)$ then $\mathfrak{m}_P = (x, y)$ and $\mathfrak{m}_P^2 = (x^2, xy, y^2)$. Since $x = \frac{1}{2}(y^2 - x^3) \in \mathfrak{m}_P^2$ (this also tells us $\operatorname{ord}_P(x) \geqslant 2$), $\mathfrak{m}_P = (x, y) = (y)$ (in the local ring at P). Thus, $\operatorname{ord}_P(y) = 1$. Now $y^2 = (x^2 + 2)x$ where $x^2 + 2 \neq 0$ at P which means it's a unit in the local ring, $x = (x^2 + 2)^{-1} y^2$ and thus

$$\operatorname{ord}_P(x) = \operatorname{ord}_P(\text{some unit}) + 2 \operatorname{ord}_P(y) = 2$$

where the order of unit must be zero by definition (otherwise $\mathfrak{m}_P$ wouldn't be maximal). Finally for $2y^2 - 3x = 2x^3 + x = (2x^2 + 1)x$, we have

$$\operatorname{ord}_P(2y^2 - 3x) = \operatorname{ord}_P(\text{some unit}) + \operatorname{ord}_P(x) = 2$$

where the equality holds since $2x^2 + 1 \neq 0$ at $P = (0,0)$, i.e., $2x^2 + 1$ is a unit.

Let k be a field of characteristic $p > 0$.

Lemma 5.2.2. *Given curve C/k and $t \in k(C)$ a uniformizer at a smooth $P \in C(k)$. Then $k(C)$ is a finite separable extension of $k(t)$.*

Proof. Since $k(C)$ is a finitely generated k-algebra, Zaraski's lemma ensures it's a finite extension of k. Clearly $k(t)$ has transcendence degree 1 ($t \notin k$ otherwise $\operatorname{ord}_P t = 0$ for all $P \in C$). Now as the transcendence degree of $k(C)/k$ is $\dim C = 1$, $\operatorname{trdeg} k(C)/k(t) = 0$, meaning $k(C)$ is an algebraic extension of $k(t)$.

Take any $x \in k(C)$ and we aim to show x is separable over $k(t)$. Since $k(C)$ is algebraic, there is some $\Phi(X, T) \in k[X, T]$ such that $\Phi(x, t) = 0$. Suppose further that Φ has minimal degree over $k(t)$.

If there is some term $a_{ij} T^i X^j$ in Φ where $p \nmid j$, then clearly $\partial \Phi(t, X)/\partial X$ is nonzero, meaning x is separable.

It remains to check when $\Phi(T, X) = \Psi(T, X^P)$ for some polynomial Ψ. Write

$$\Phi = \Psi(T, X^p) = \sum_{k=0}^{p-1} \left(\sum_{i,j} b_{ijk} T^{ip} X^{jp} \right) T^k$$

Since k is perfect of characteristic $p > 0$, every element of k is a pth power. Thus, define $c_{ijk}^p = b_{ijk}$ and thus

$$\sum_{i,j} b_{ijk} T^{ip} X^{jp} = \sum_{i,j} (c_{ijk} X^i T^j)^p = \left(\sum_{i,j} c_{ijk} X^i T^j \right)^p = \varphi_k(T, X)^p$$

Evaluate the order of each summand:

$$\operatorname{ord}_P(\varphi_k(t,x)^p t^k) = p \operatorname{ord}_P(\cdots) + k \operatorname{ord}_P(t) \equiv k \pmod p$$

which means they have different orders, and thus must all vanish as $\Phi(t,x) = 0$. There must exist some k such that φ_k contains X and $\varphi_k(t,x) = 0$. Yet $\Phi(t,X)$ is minimal and $\deg \varphi_k(t,X)^p \leqslant \deg \Phi(t,X)$ so we get a contradiction. □

Definition 5.2.3. For any point P on a curve C and any $f \in K(C)$, if $\operatorname{ord}_P(f) \geqslant 0$ then f is *regular at* P. If $\operatorname{ord}_P(f) > 0$ then f has *a zero of order* $\operatorname{ord}_P(f)$ *at* P; if $\operatorname{ord}_P(f) < 0$ then f has *a pole of order* $-\operatorname{ord}_P(f)$ *at* P

Remark 5.2.3. If $f = g/h$ is regular at P, then f corresponds to some element of $K[C]_P$, meaning there exist $g', h' \in K[C]$ such that $h' \neq 0$ near P and thus f is regular at P in the usual sense.

The order ord_P at any point P satisfies a very important property, which is an essential part of our algebraic geometry machine.

Theorem 5.2.1. *Let C be a curve and $f \in K(C)$. Then the set $\{P \in C : \operatorname{ord}_P(f) \neq 0\}$ is finite. Furthermore, if f has no poles on C, then $f \in K$.*

Proof. The proof of this theorem by elementary variety theory is rather long and complicated. A short proof using schemes is available in [Har10], II.6.1. □

5.3 Morphisms of curves

Let C_1, C_2 be two (smooth) curves. A rational map $\varphi : C_1 \to C_2$ is a morphism if it's regular at every point on C_1. We present a small lemma as an application of ord. The term regular

Lemma 5.3.1. *Any rational map $\varphi = [f_0 : \cdots : f_m] : C \to V$ from a (smooth) curve to a variety $V \subseteq \mathbb{P}^m$ is a morphism.*

Proof. It suffices to show that for all $P \in C$, there is some $g \in K(C)$ such that each gf_i is regular at P. Let $m = \min_i \operatorname{ord}_P(f_i)$. As Remark 5.2.2 suggests, there is a uniformizer at P, say t, such that $\operatorname{ord}_P(t) = 1$. Then $\operatorname{ord}_P(t^{-m} f_i) \geqslant 0$ for all i, completing the proof. □

If C_1/k and C_2/k, a nonconstant rational map $\varphi : C_1 \to C_2$ defined over k induces an injective pullback $\varphi^* : k(C_2) \to k(C_1)$ fixing k. We quote the following theorem:

Theorem 5.3.1. *Given curves C_1/k and C_2/k, the following statements hold:*

(i) *For any nonconstant rational map φ, $k(C_1)$ is a finite extension of the pullback of $k(C_2)$, that is, $[k(C_1) : \varphi^* k(C_2)] < \infty$.*

(ii) *For any injective field homomorphism $\psi : k(C_2) \to k(C_1)$ fixing k, there is a nonconstant rational map $\varphi : C_1 \to C_2$ such that $\varphi^* = \psi$.*

Proof. The proof is omitted. □

Definition 5.3.1. Suppose $\varphi : C_1 \to C_2$ is a rational map. If φ is constant we define the *degree of* φ, $\deg \varphi$, to be 0 and if φ is nonconstant, then we define

$$\deg \varphi = [k(C_1) : \varphi^* k(C_2)]$$

In particular, a rational map φ is *separable, inseparable or purely inseparable* if the extension $k(C_1)/\varphi^* k(C_2)$ is (see definitions in Section 1.1).

Definition 5.3.2. We define the *ramification index of φ at P* to be the order

$$e_\varphi(P) = \operatorname{ord}_P \left(\varphi^* t_{\varphi(P)}\right)$$

where $t_{\varphi(P)}$ is any uniformizer at $\varphi(P)$. Note: the choice of t does not matter.

Here are some general facts about the ramification index:

Lemma 5.3.2. *Suppose $\varphi : C_1 \to C_2$ is a nonconstant morphism, then*

(i) *For all $Q \in C_2$,*

$$\sum_{P \in \varphi^{-1}(Q)} e_\varphi(P) = \deg \varphi$$

(ii) *For all but finitely many $Q \in C_2$,*

$$\#\varphi^{-1}(Q) = \deg_s \varphi$$

where $\deg_s$ is the separable degree

$$[\varphi^* k(C_2)^{\text{sep}} : \varphi^* k(C_2)]$$

from Theorem 1.1.3

Furthermore, if $\psi : C_2 \to C_3$ is another nonconstant map,

$$e_{\psi\circ\varphi}(P) = e_\psi(\varphi(P)) e_\varphi(P)$$

Proof. The first two statements are nontrivial and can be found in [Har10].

For the last statement, let t_1, t_2 be uniformizers at at $\varphi(P)$ and $\psi(\varphi(P))$ respectively. Then by definition

$$\operatorname{ord}_{\varphi(P)}\left(t_1^{e_\psi(\varphi(P))}\right) = e_\psi(\varphi(P)) = \operatorname{ord}_{\varphi(P)}(\psi^* t_2)$$

and thus,

$$e_{\varphi\circ\varphi}(P) = \operatorname{ord}_P((\psi\circ\varphi)^* t_2) = \operatorname{ord}_{\varphi(P)}(\varphi^* t_1^{e_\psi(\varphi(P))}) = e_\psi(\varphi(P))e_\varphi(P)$$

which completes the proof. □

5.4 The Frobenius map

On a field K of characteristic $p > 0$, we have an extremely important map — *the Frobenius endomorphism* $F : x \mapsto x^p$. It is clear that $F(x+y) = F(x) + F(y)$ since the prime p divides all $\binom{p}{k}$ with $0 < k < p$.

Remark 5.4.1. The invariant set of the nth iterate of the Frobenius endomorphism (that is, F^n) is simply $\mathbb{F}_{p^n}$. This property is one of the most essential "reasons" Weil conjectures holds.

Now for any curve C/k with $\operatorname{char} k = p > 0$, we can define a new curve $C^{(q)}$ for any $q = p^m$ to be the zero locus of

$$I = \{f^{(q)} : f \in \mathbb{I}(C)\}$$

where $f^{(q)}$ is simply the polynomial resulting from raising the coefficients of f to the qth power.

Definition 5.4.1. Then the map $\varphi : C \to C^{(q)}$ defined by $\varphi = [F^m : \cdots : F^m]$ is called the *qth-power Frobenius map.*

It is easy to check that the image of φ is indeed inside $C^{(q)}$. Say $f(P) = 0$, then

$$f^{(q)}(\varphi(P)) = f^{(q)}(x_0^q, \ldots, x_n^q) = (f(P))^q = 0$$

as k is of characteristic p. The proof of the following theorem is omitted.

Theorem 5.4.1. *We have* $\varphi^* k(C^{(q)}) = k(C)^q$ *which means* φ *is purely inseparable. Furthermore,* $\deg\varphi = p$.

Corollary 5.4.1. *Let $\psi : C_1 \to C_2$ be a map between curves over a field of* char $=$ $p > 0$. *Write $q = \deg_i \psi$. Then there exists separable $\lambda : C_1^{(q)} \to C_2$ such that*

$$\psi = \lambda \circ \varphi_q$$

where φ_q is the qth power Frobenius map.

Proof. Let k^{sep} be the separable closure of $\psi^* k(C_2)$ in $k(C_2)$. Then $k(C_1)/k^{\text{sep}}$ is purely inseparable of degree q which means $k(C_1)^q \subseteq k^{\text{sep}}$. But by Theorem 5.4.1,

$$\varphi_q^* k(C_1^{(q)}) = k(C_1)^q, \quad [k(C_1) : \varphi_q^* k(C_1^{(q)})] = q$$

so we must have $k^{\text{sep}} = \varphi_q^* k(C_1^{(q)})$, which means the extensions satisfy

$$k(C_1)/\varphi_q^* k(C_1^{(q)})/\psi^* k(C_2)$$

where $\varphi_q^* k(C_1^{(q)})/\psi^* k(C_2)$ is separable. From (ii) in Theorem 5.3.1, there is a λ separable such that $\lambda \circ \varphi_q = \psi$. □

5.5 Weil divisors and the Picard groups

In this section we introduce an extremely important algebro-geometric tool which would help us in defining and proving many important results. Let C be any curve.

Definition 5.5.1. A *Weil divisor D on C* is a formal sum

$$D = \sum_{P \in C} n_P(P)$$

where only finitely many $n_P \in \mathbb{Z}$ are nonzero. The brackets around each point P only emphasizes that the point here is considered as a part of the formal sum, not an actual point.

The additive abelian group consisting of all Weil divisors on C is called the *divisor group of C*, denoted by $\text{Div}(C)$. The addition inside this group is just the coefficients-wise addition.

The Galois group $\text{Gal}(K/k)$ acts on D by

$$D^\sigma = \sum_{P \in C} n_P(P^\sigma)$$

We say that a divisor D is *defined over k* if $D^\sigma = D$ for all $\sigma \in \text{Gal}(K/k)$ and such divisors form a subgroup $\text{Div}_k(C)$.

Definition 5.5.2. We define the *degree of a divisor D* to be

$$\deg D = \sum_{p \in C} n_P$$

which makes sense since there are only finitely nonzero n_P. The subgroup formed by all divisors of degree 0 is denoted by $\mathrm{Div}^0(C)$.

Remark 5.5.1. By definition, $\deg(D_1 + D_2) = \deg D_1 + \deg D_2$ and $\deg(-D) = -\deg D$.

Example 5.5.1. Here we present a trivial example to assist understanding the idea of a formal sum. Say P, Q, S are three distinct points in C. Then let $D_1 = 2(P)+5(Q)$ and $D_2 = -(Q) - 7(S)$. Then $D_1 + D_2$ is nothing else but $2(P) + 4(Q) - (S)$. They do not need to have a specific meaning now. The degree of D_1 is $2 + 5 = 7$.

In the following sections we will refer to Weil divisors as divisors. Given some $f \in K(C)$, we see in Theorem 5.2.1, there are only finitely many points $P \in C$ such $\mathrm{ord}_P(f) \neq 0$. Therefore, the order valuation can be used to define a special type of divisors:

Definition 5.5.3. For any $f \neq 0 \in K(C)$, the *divisor associated to f* is

$$\mathrm{div}(f) = \sum_{p \in C} \mathrm{ord}_P(f)(P).$$

A divisor D on C is a *principal divisor* if there is some $f \neq 0 \in K(C)$ such that $D = \mathrm{div}(f)$.

Remark 5.5.2. Obviously for all $\sigma \in \mathrm{Gal}(K/k)$, we have

$$\begin{aligned}(\mathrm{div}(f))^\sigma &= \sum \mathrm{ord}_P(f)(P^\sigma)\\ &= \sum \mathrm{ord}_{P^\sigma}(f^\sigma)(P^\sigma)\\ &= \sum \mathrm{ord}_P(f^s)(P) = \mathrm{div}(f^\sigma)\end{aligned}$$

where the second equality comes from the fact that $f^\sigma(Q^\sigma) = (f(Q))^\sigma$ for all $Q \in C$ so the order is invariant under σ.

Clearly if $f \in k(C)$, $f = f^\sigma$ so $\mathrm{div}(f) \in \mathrm{Div}_k(C)$.

Lemma 5.5.1. *For any $f \neq 0 \in K(C)$,*

(i) $\operatorname{div} f = 0$ *if and only if* $f \in K^\times$.

(ii) $\deg \operatorname{div}(f) = 0$.

Two divisors D_1, D_2 are equivalent $D_1 \sim D_2$ if and only if $D_1 - D_2$ is a principal divisor. This equivalence relation gives us a quotient $\operatorname{Div}(C)/\sim$. We denote this group by $\operatorname{Pic}(C)$ and call it the *Picard group of* C. Similarly we denote by $\operatorname{Pic}^0(C)$ the *degree*-0 *part of the Picard group of* C, that is, $\operatorname{Div}^0(C)/\sim$.

Given a nonconstant map $\varphi : C_1 \to C_2$, we can define the pullback and pushforward map of φ between the divisor groups of C_i as

$$\varphi^* : \operatorname{Div}(C_2) \to \operatorname{Div}(C_2), \quad \varphi^*(Q) = \sum_{P \in \varphi^{-1}(Q)} e_\varphi(P)(P)$$

and

$$\varphi_* : \operatorname{Div}(C_1) \to \operatorname{Div}(C_2), \quad \varphi_*(P) \mapsto (\varphi(P)),$$

and extend them linearly.

Lemma 5.5.2. *The pushforward map* φ_* *preserves principal divisors and divisors of degree* 0. *Therefore it defines a homomorphism* $\varphi_* : \operatorname{Pic}^0(C_1) \to \operatorname{Pic}^0(C_2)$.

5.6 Differentials and canonical divisors

The definition we present for differential forms is extremely simple, but it will do the job for us.

Let C be a curve defined on K/k. The *space of differential forms on* C Ω_C is defined to be the $K(C)$-vector space generated by all elements satisfying the following definition:

Definition 5.6.1. A *differential form on* C is an element generated by symbols dx where $x \in K(C)$ such that

(i) $d(x + y) = dx + dy$.

(ii) $d(xy) = xdy + ydx$.

(iii) $dr = 0$ for all $r \in K$.

Remark 5.6.1. Silverman's text contains a typo — Ω_C is not only a K-vector space but also a $K(C)$-vector space.

Every morphism $\varphi : C_1 \to C_2$ induces a pullback of differential forms $\varphi^* : \Omega_2 \to \Omega_1$ defined by

$$\sum f_i dx_i \mapsto \sum \varphi^* f_i d\left(\varphi^* x_i\right)$$

which gives a separability test of φ (which we won't prove):

Lemma 5.6.1. (i) *The space Ω_C is one-dimensional over $K(C)$ for any curve C.*

(ii) *A form dx is a basis of Ω_C if and only if $K(C)/K(x)$ is separable.*

(iii) *Suppose $\varphi : C_1 \to C_2$ is nonconstant, then φ is separable if and only if $\varphi^* : \Omega_2 \to \Omega_1$ is an injective map.*

Suppose $\operatorname{char} k > 0$. Then we have the following theorem.

Theorem 5.6.1. *Let C be a curve, $P \in C$ and $t \in K(C)$ a uniformizer at P. Then for every $\omega \in \Omega_C$, there is a unique $g \in K(C)$, denoted by ω/dt, such that $\omega = gdt$. Furthermore, $\operatorname{ord}_P(g)$ is independent of the choice of t and we denote this quantity by $\operatorname{ord}_P(\omega)$. In particular, $\operatorname{ord}_P(\omega) = 0$ for all but finitely many $P \in C$.*

Proof. The proof of the first statement is easy. By Lemma 5.2.2, $K(C)/K(t)$ is separable so by (ii) in Lemma 5.6.1, dt generates Ω_C and the statement follows. The proofs of the other two statements are omitted. □

Definition 5.6.2. For any $\omega \neq 0 \in \Omega_C$, the divisor associated to ω/dt is called a *canonical divisor*, denoted by $\operatorname{div}(\omega)$. As for rational functions, if $\operatorname{ord}_P(\omega) \geqslant 0$ for all $P \in C$ then we say ω is *holomorphic* and we say it's nonvanishing if $\operatorname{ord}_P(\omega)$ for all $P \in C$.

Remark 5.6.2. All canonical divisors are equivalent in $\operatorname{Pic}(C)$. Take nonzero $\omega_1, \omega_2 \in \Omega_C$, since the latter space is one-dimensional, we have some $f \in K(C)$ such that $\omega_1 = f\omega_2$. In this case $\operatorname{ord}_P(\omega_1) = \operatorname{ord}_P(f) + \operatorname{ord}_P(\omega_2)$ and thus by definition $\operatorname{div}(\omega_1) = \operatorname{div}(f) + \operatorname{div}(\omega_2)$.

5.7 The Riemann-Roch theorem for curves

In this section, we will state the superbly powerful Riemann-Roch theorem without introducing the concept of differentials. This means some objects associated to a curve will not be defined but some of their special properties will be provided.

Given a curve C and a divisor D on C, we say D is *positive* if all $n_P \geqslant 0$. We denote this by $D \geqslant 0$. Given two divisors we write $D_1 \geqslant D_2$ if $D_1 - D_2 \geqslant 0$.

Remark 5.7.1. The definition above might not be so trivial as they seem to be. Given any $f \neq 0 \in K(C)$, if it is regular everywhere except at finitely many points $P_1, \ldots, P_n$ with poles of order less than or equal to $a_1, \ldots, a_n$ (which means $\mathrm{ord}_P(f) \geqslant 0$ for $P \neq P_i$ and $\mathrm{ord}_{P_i}(f) \geqslant -a_i$), we can write

$$\mathrm{div}(f) \geqslant \sum_{i \leqslant n} -a_i(P_i)$$

Similarly, if f has a zero at Q, then one may write $\mathrm{div}(f) \geqslant (Q)$, which is quite convenient.

Also, it is clear that if $D_1 \geqslant D_2$, then $\deg D_1 \geqslant \deg D_2$.

Definition 5.7.1. For a divisor D, define a K-vector space:

$$\mathcal{L}(D) = \{f \neq 0 \in K(C) : \mathrm{div}(f) \geqslant -D\} \cup \{0\}$$

This vector space is actually finite-dimensional (nontrivial result; proof omitted), and we write

$$l(D) = \dim_K \mathcal{L}(D).$$

Lemma 5.7.1. *For any $D \in \mathrm{Div}(C)$,*

(i) *If $\deg D < 0$ then $\mathcal{L}(D) = 0$.*

(ii) *For another $D' \in \mathrm{Div}(C)$, if $D \equiv D'$ in $\mathrm{Pic}(C)$, then $\mathcal{L}(D) \cong \mathcal{L}(D')$ and as a consequence $l(D) = l(D')$.*

Proof. For (i) we quote Lemma 5.5.1. Since $\deg D < 0$ and for any nonzero $f \in K(C)$, $f \in \mathcal{L}(C)$ if $\deg \mathrm{div}(f) \geqslant -\deg D > 0$. Yet the LHS is zero, so $\mathcal{L}(C) = 0$.

For (ii), suppose $D - D' = \mathrm{div}(g)$. We have an isomorphism

$$\alpha : \mathcal{L}(D) \to \mathcal{L}(D')$$

defined by $f \mapsto fg$ (one only needs to check that this map and its inverse $f \mapsto f/g$ are both well-defined, which is an easy argument on orders). □

Let K_C be a canonical divisor. By Remark 5.6.2, when dealing with the $\mathcal{L}$ space of these divisors, we can always use the notation K_C to represent any canonical divisor on C as $l(K_C)$ are always the same.

Theorem 5.7.1 (Riemann-Roch)**.** *Let C be a curve and K_C the canonical divisor on C. There is an integer $g \geqslant 0$ called the* genus of C *such that for any $D \in \mathrm{Div}(C)$,*

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

Proof. Proof omitted. See [Har10] for example. □

Remark 5.7.2. The term $l(K_C - D)$ is sometimes called the correction term. Since $l(K_C - D) \geqslant 0$ for any D, we have

$$l(D) \geqslant \deg D - g + 1$$

which is called Riemann's inequality.

Corollary 5.7.1. *The followings hold:*

(i) $l(K_C) = g$.

(ii) $\deg K_C = 2g - 2$ *(which is* $-\chi$ *where* χ *is the Euler characteristic of* C*).*

(iii) *If* $\deg D > 2g - 2$, *then* $l(D) = \deg D - g + 1$

Proof. For (i) take $D = 0$ then by Remark 5.7.1 any $f \in \mathcal{L}(D)$ has no poles, i.e., they are just constants by Theorem 5.2.1. Thus, $\mathcal{L}(D) = K$ and therefore $l(D) = \dim_K K = 1$. Plugging this into Riemann-Roch we get the result.

For (ii) take $D = K_C$. Then $l(D) = g$ and thus $l(D) - l(0) = \deg K_C - g + 1$. Since $l(0) = 1$ we get $\deg K_C = 2g - 2$.

For (iii), $\deg D > 2g - 2$ together with (ii) suggests $\deg(K_C - D) < 0$. Thus, $\mathcal{L}(K_C - D) = 0$ by Lemma 5.7.1. This means $l(D) = \deg D - g + 1$. □

6 More on Elliptic Curves

6.1 Curves of genus one

In this section we present a more abstract definition of elliptic curves, and show that this definition is equivalent to the one using Weierstrass normal forms.

Definition 6.1.1. An *elliptic curve* is a pair $(E, \mathcal{O})$ where E is a (smooth) curve of genus 1 and $\mathcal{O} \in E$. We say that E *is defined over* k if E/k and $\mathcal{O} \in E(k)$.

Remark 6.1.1. The selected k-rational base point $\mathcal{O}$ is extremely important in the definition of elliptic curves. There are several reasons for taking it: first, many smooth projective curves of genus one does NOT have rational points. For example, the curve $y^2 = 1 - 17x^4$ has no rational points (and it violates the Hasse principle) over $\mathbb{Q}$ [Poo99]. Second, we need the rationality of this base point to generate the $\mathcal{L}$-space of $n(\mathcal{O})$ with elements in $k(C)$, see the proof of (i) in Theorem 6.1.1; we want that, for all elliptic curves defined above, there is some Weierstrass equation with k-rational coefficients.

Theorem 6.1.1. *Suppose E/k is an elliptic curve with a base point $\mathcal{O}$, then*

(i) *There exists $f, g \in k(E)$ such that the map*

$$\varphi : E \to \mathbb{P}^2, \quad P \mapsto [f(P) : g(P) : 1]$$

is an isomorphism onto a curve given by some Weierstrass equation

$$C : y^2 + a_1 xy + a_3 y = x^3 + a_2 x + a_4 x + a_6$$

with k-rational coefficients and $\varphi(\mathcal{O}) = [0 : 1 : 0]$. In this case, f, g are called the Weierstrass coordinate of E.

(ii) *Any two Weierstrass equations of E are related by a linear change of variables.*

(iii) *All curves defined by Weierstrass equations with k-rational coefficients are elliptic curves with the base point $[0 : 1 : 0]$.*

Proof. We only prove (i) partially and omit the remaining.

(i) For E, $2g - 2 = 0$ so $\deg n(\mathcal{O}) = n > 2g - 2$ for all $n \geqslant 1$. Then by Corollary 5.7.1 (iii), $l(n(\mathcal{O})) = n$. Let $\{1, f\} \subseteq k(E)$ (we can take the fact that if $D \in \operatorname{Div}_k(C)$ then $\mathcal{L}(D)$ has a basis of elements in $k(C)$) be a basis of $\mathcal{L}(2(\mathcal{O}))$, and extending it to a basis $\{1, f, g\}$ of $\mathcal{L}(3(\mathcal{O}))$. Here $\operatorname{ord}_{\mathcal{O}}(f) = -2$ and $\operatorname{ord}_{\mathcal{O}}(g) = -3$ (proof omitted). Now f^2, f^3, fg, g^2 all have order $\geqslant -6$ at $\mathcal{O}$, so they are all in $\mathcal{L}(6(\mathcal{O}))$. But then we would have seven functions $\{1, f, g, f^2, f^3, fg, g^2\}$ in a K-vector space of dimension 6 (so its dimension over k must be at most 6). Thus, there are $A_1, \ldots, A_7 \in k$ such that

$$A_1 + A_2 f + A_3 g + A_4 f^2 + A_5 fg + A_6 g^2 + A_7 f^3 = 0$$

where $A_6, A_7 \neq 0$ or else all elements remaining will have different orders at $\mathcal{O}$. Replace f, g by $-A_6 A_7 f$ and $A_6 A_7^2 g$,

$$A_1 - A_2 A_6 A_7 f + A_3 A_6 A_7^2 g - A_4 A_6^2 A_7^2 f^2 - A_5 A_6^2 A_7^3 fg + A_6^3 A_7^4 g^2 - A_6^3 A_7^4 f^3 = 0$$

and rescaling gives us the map

$$\varphi : P \mapsto [f(P) : g(P) : 1]$$

under which $\operatorname{im} \varphi$ is contained in some zero locus V of an Weierstrass equation. However since φ is nonconstant and it's a morphism as E is smooth, it must be surjective (standard algebraic geometry result). Thus, $\operatorname{im}\varphi = V$ is defined by an Weierstrass equation.

By definition, the pullback of $k(C)$ under φ is just $k(f, g)$. We claim that $[k(E) : k(x, y)] = \deg\varphi = 1$. Since the orders of f, g at $\mathcal{O}$ are $-2, -3$ respectively, $[k(E) : k(f)] = 2$, $[k(E) : k(g)] = 3$. This means $\deg\varphi$ must divide two coprime numbers and thus it's one. We will take for granted that $\operatorname{im}\varphi$ is smooth, and morphisms between smooth curves of degree 1 are isomorphism. Thus, φ is an isomorphism.

(ii) Suppose $\{f, g\}, \{f', g'\}$ are two sets of Weierstrass coordinates, then $\{1, f\}$, $\{1, f'\}$ ($\{1, f, g\}$,$\{1, f', g'\}$) are both bases of $\mathcal{L}(2(\mathcal{O}))$ ($\mathcal{L}(3(\mathcal{O}))$). We therefore have $u_1, u_2 \in k^\times$ and $r, t, s_2 \in k$ such that

$$x = u_1x' + r, \quad y = u_2y' + s_2x' + t.$$

Yet, x, y satisfy the Weierstrass equation so $u_1^3 = u_2^2$ and after a change of variables, we get the result.

(iii) Recall that every curve defined by a Weierstrass equation we have a nonzero, regular, nonvanishing differential form called the invariant differential:

$$\omega = \frac{dx}{2y - a_1x + a_3}$$

Since we know that it's regular and nonvanishing, we get a canonical divisor $K_E = \operatorname{div}(\omega) = 0$. Thus, by (ii) in Corollary 5.7.1, we get

$$0 = \deg K_E = 2g - 2$$

which means the curve E has genus one, completing the proof. □

6.2 The algebraic group law

Recall in Section 5.5, we defined something call the Picard group of a curve, by modding out principal divisors from the group of divisors. In this section we use the subgroup $\operatorname{Pic}^0(E)$ to derive a group structure on E. To prepare for the main construction, we start with an easy lemma

Lemma 6.2.1. *Suppose E is an elliptic curve. Then for any two points $P, Q \in E$, $(P) \sim (Q)$ if and only if $P = Q$.*

Proof. Let $f \neq 0 \in K(C)$ such that $\operatorname{div}(f) = (P) - (Q)$. Clearly $\operatorname{div}(f) \geqslant -(Q)$ so $\operatorname{div}(f) \in \mathcal{L}((Q))$. But since the genus of E is $g = 1$, $\deg(Q) = 1 > 2g - 2$. Thus, by Corollary 5.7.1 (iii), $l((Q)) = \deg(Q) = 1$. Therefore, as $1 \in \mathcal{L}((Q))$, $f \in K$ and $\operatorname{div}(f) = 0$. This means $P = Q$ (otherwise the formal sum cannot cancel). □

Consider any divisor $D \in \mathrm{Div}^0(E)$ of degree 0. We have $l(D + (\mathcal{O})) = \deg(D + (\mathcal{O})) = 1$ by Corollary 5.7.1 (iii). Let f be a nonzero element of $K(E)$ that spans $\mathcal{L}(D+(\mathcal{O}))$. Then we have $\mathrm{div}(f) \geqslant -D-(\mathcal{O})$. But by Lemma 5.5.1, $\deg \mathrm{div}(f) = 0$, we have some $P \in E$ such that $\mathrm{div}(f) = -D - (\mathcal{O}) + (P)$ To deduce the last statement, We must think about the formal sum. The inequality above tells us that the coefficients in $\mathrm{div}\, f$ before (Q) and each term in D must be larger than -1 and the coefficient of each term in $-D$; but the coefficient before $\mathcal{O}$ in $\mathrm{div}(f)$ cannot be positive, otherwise we cannot cancel it in the degree, as the other coefficients must be nonnegative. Thus the degree of $\mathrm{div}(f) = 0$ suggests that there is one single point (or else the degree of the part other than $-D - (\mathcal{O})$ would be ¿1, which is impossible to cancel in $\deg \mathrm{div}(f)$) such that $\mathrm{div}(f) = -D - (\mathcal{O}) + (P)$ (it could be $\mathcal{O}$ of course). Then if P' is another such point, we have $(P') \sim D + (\mathcal{O}) \sim (P)$ which by Lemma 6.2.1 gives $P = P'$.

Let $\sigma : \mathrm{Div}^0(E) \to E$ be the map sending D to the unique point P found above.

Theorem 6.2.1. *The map σ induces a bijection $\sigma : \mathrm{Pic}^0(E) \to E$, with its inverse being $\kappa : E \to \mathrm{Pic}^0(E)$ defined by $P \mapsto [(P) - (\mathcal{O})]$. Therefore we can impose E with a group structure by defining*

$$P + Q = \kappa^{-1}(\kappa(P) + \kappa(Q)).$$

Proof. For any point $P \in E$, the divisor $(P) - (\mathcal{O})$ has degree 0. Therefore by construction $\sigma((P) - (\mathcal{O})) = P$, which means σ is surjective.

We now prove that $\sigma(D_1) = \sigma(D_2)$ if and only if $D_1 \sim D_2$. Suppose $P = \sigma(D_1) = \sigma(D_2)$. Then $D_i \sim (P) - (\mathcal{O})$ imply $D_1 - D_2 \sim (P) - (P) = 0$ and thus $D_1 \sim D_2$. Conversely if $D_1 \sim D_2 \sim (P) - (\mathcal{O})$ for a unique P, by definition, $\sigma(D_1) = \sigma(D_2) = P$. Thus, we have a bijection:

$$\sigma : \mathrm{Pic}^0(E) \to E$$

and the inverse map is deduced when we proved σ's surjectivity. □

Theorem 6.2.2. *The algebraic group law and the geometric group law defined on an elliptic curve are the same thing.*

Proof. It suffices to show that $\kappa(P + Q) = \kappa(P) + \kappa(Q)$ (where the first addition is the addition from the geometric group law). Let $L = \mathbb{V}(f)$ be the line passing through P, Q; let R be the third point of intersection of this line and E; let $L' = \mathbb{V}(f')$ be the line passing through $R, \mathcal{O}$. Then since $Z = 0$ intersects with E at $\mathcal{O}$ with multiplicity 3 (so that $\mathrm{ord}_{\mathcal{O}}(Z) = 3$), we have

$$\mathrm{div}(f/Z) = (P) + (Q) + (R) - 3(\mathcal{O}), \quad \mathrm{div}(f'/Z) = (R) + (P + Q) + (\mathcal{O}) - 3(\mathcal{O})$$

where we know for example $\text{ord}_P(f) = 1$ since f is a polynomial of degree 1 and the maximal ideal $\mathfrak{m}_P$ is generated by some nonconstant polynomial so we cannot have $f \in \mathfrak{m}_P^d$ for any $d > 1$. This means

$$\text{div}(f'/f) = (P+Q) - (P) - (Q) + (\mathcal{O})$$

which is principal so equivalent to 0. But in $\text{Pic}^0(E)$,

$$\kappa(P+Q) - \kappa(P) - \kappa(Q) = (P+Q) - (\mathcal{O}) - (P) + (\mathcal{O}) - (Q) + (\mathcal{O}) \equiv 0$$

which completes the proof. □

Corollary 6.2.1. *Given a divisor $D \in \text{Div}(E)$, it is principal if and only if*

$$\deg D = 0, \quad \sum [n_p]P = 0$$

where we write $D = \sum n_P(P)$.

Proof. If D is principal then by Lemma 5.5.1, $\deg D = 0$. Also, using the σ map defined in Theorem 6.2.1, we have $D \sim 0$ implies $\sigma([D]) = \mathcal{O}$ which means

$$\sum [n_P]\sigma[(P) - (\mathcal{O})] = \sum [n_P]P = \mathcal{O}$$

where we used the definition that $\sigma[(P) - (\mathcal{O})] = P$.

Now if $D \in \text{Div}^0(E)$ and $\sum [n_P]P = \mathcal{O}$, then $\sigma(D) = \mathcal{O}$ and thus $D \sim 0$. □

Lemma 6.2.2. *The addition and negation map on an elliptic curve are morphisms of elliptic curves.*

Proof. Simply use the explicit formulas. □

7 Constructions on Elliptic Curves

In this section we talk about several important objects on elliptic curves.

7.1 Isogenies

Definition 7.1.1. Given two elliptic curves E_1, E_2, a morphism $\varphi : E_1 \to E_2$ is an *isogeny* if it preserves the base point, that is, $\varphi(\mathcal{O}) = \mathcal{O}$. Two elliptic curves are called *isogenous* if there is a nonconstant isogeny from E_1 to E_2.

Remark 7.1.1. If $\varphi \neq [0]$ (where $[0]$ is the trivial isogeny sending everything to $\mathcal{O}$) is an isogeny, then φ is surjective. We define the degrees of φ as before. We define $\deg[0] = 0$ so that we would have $\deg(\psi \circ \varphi) = \deg \psi \deg \varphi$.

Let the Hom-space of elliptic curves to be $\operatorname{Hom}(E_1, E_2) = \{\text{isogeny } : E_1 \to E_2\}$ and $\operatorname{End}(E) = \operatorname{Hom}(E_1, E_2)$.

Definition 7.1.2. The *multiplication-by-m isogeny* $[m]$ is the map sending P to the sum of $|m|$ numbers of $\operatorname{sgn}(m)P$.

The proof of the following lemma is tedious so it is omitted.

Lemma 7.1.1. *The map $[m]$ is nonconstant for $m > 0$.*

The abelian group $\operatorname{Hom}(E_1, E_2)$ forms a $\mathbb{Z}$-module by defining $m\varphi = [m] \circ \varphi$. Then if $m\varphi = 0$, $0 = \deg m\varphi = \deg[m] \deg \varphi$. Now if $\deg \varphi \neq 0$ (which means $\varphi = [0]$) then $\deg[m] = 0$ which implies $m = 0$ as $[m]$ is nonconstant for $m > 0$. Thus, $\operatorname{Hom}(E_1, E_2)$ is torsion free. Using the same argument we can show that $\operatorname{End}(E)$ is an integral domain of characteristic 0.

Definition 7.1.3. The *m-torsion subgroup* of E is denoted by $E[m]$. The *torsion subgroup of E* is the union

$$E_{\text{tor}} = \bigcup_{m \geqslant 1} E[m]$$

We use the notation $E[m](k)$ and $E_{\text{tor}}(k)$ to denote the corresponding rational torsion points.

Remark 7.1.2. If a point $P \neq \mathcal{O}$ has order 2, then $[2]P = \mathcal{O}$, which is equivalent to $P = -P$, so $(x, y) = -(x, y) = (x, -y)$, indicating $y = 0$. This shows that the rational points of order 2 are given by $y = 0$, namely $\{\mathcal{O}, (x_1, 0), (x_2, 0), (x_3, 0)\}$, where $x_i \in K$ are (distinct) solutions to the elliptic curve's Weierstrass equation.

If a point $P \neq \mathcal{O}$ has order 3, then $[3]P = \mathcal{O}$, which is equivalent to $[2]P = [-1]P$. This happens if and only if the x-coordinate of P satisfies $x(P) = x([2]P)$. Using the explicit duplication formula, it can be shown that every elliptic curve has exactly nine points of order dividing three, forming a group isomorphic to $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$.

Remark 7.1.3. If $k = \mathbb{F}_q$ and E/k, then the Frobenius map defined in Definition 5.4.1 is an endomorphism since $E^{(q)} = E$ for all $q = p^r$, so it's now called the *Frobenius endomorphism* and denoted by φ_q. The fixed points of this endomorphism are precisely $E(\mathbb{F}_q)$.

Lemma 7.1.2. *Every isogeny $\varphi : E_1 \to E_2$ is a homomorphism of groups.*

Proof. If $\varphi = [0]$ then we are done. Suppose $\varphi \neq [0]$. Then by Lemma 5.5.2, there is a homomorphism $\varphi_* : \mathrm{Pic}^0(E_1) \to \mathrm{Pic}^0(E_2)$ defined by

$$\left[\sum n_P(P)\right] \mapsto \left[\sum n_P(\varphi(P))\right]$$

Recall the isomorphisms $\kappa_i : E_i \to \mathrm{Pic}^0(E_i)$ defined by $P \mapsto [(P) - (\mathcal{O})]$. They satisfy

$$\varphi_*\kappa_1(P) = [(\varphi(P)) - (\varphi(\mathcal{O}))] = [(\varphi(P)) - (\mathcal{O})] = \kappa_2(\varphi(P))$$

since $\varphi(\mathcal{O}) = \mathcal{O}$. Therefore $\varphi = \kappa_2^{-1} \circ \varphi_* \circ \kappa_1$ is a group homomorphism. □

The kernel $\ker\varphi = \varphi^{-1}(\mathcal{O})$ is therefore a subgroup of E_1 and finite by Lemma 5.3.2.

There are two important results on the size of kernel stated below. The proofs of these two results require some complicated constructions that we do not want to know in this report. Therefore, we will take the theorems for granted.

Theorem 7.1.1. *Let $\varphi : E_1 \to E_2$ be an isogeny. Then for all $Q \in E_2$, $\#\varphi^{-1}(Q) = \deg_s \varphi$ and for all $P \in E_1$, $e_\varphi(P) = \deg_i \varphi$. In particular, if φ is separable, $\#\ker\varphi = \deg\varphi$.*

Theorem 7.1.2. *If φ_q is the qth-power Frobenius map on some elliptic curve $E/\mathbb{F}_q$ of characteristic $p > 0$, then all maps $m + n\varphi_q : E \to E$ where $p \nmid m$ are separable.*

Remark 7.1.4. By Theorem 7.1.2, $1 - \varphi_q$ is always separable. Therefore, the fixed points of φ_q, $\{P \in E : (1 - \varphi_q)(P) = \mathcal{O}\}$, has size $\deg(1 - \varphi_q)$.

Remark 7.1.5. For a fixed point $Q \in E$, we define the map $\tau_Q : P \mapsto P + Q$ to be the *translation by* Q morphism. For any morphism $F : E_1 \to E_2$ of elliptic curves, we have

$$\varphi = \tau_{-F(\mathcal{O})} \circ F \in \mathrm{Hom}(E_1, E_2)$$

as $\varphi(\mathcal{O}) = F(\mathcal{O}) - F(\mathcal{O}) = \mathcal{O}$. Therefore, every morphism can be expressed as a composition of a translation and an isogeny.

Still without a proof, we have the following decomposition theorem:

Theorem 7.1.3. *Suppose $\varphi : E_1 \to E_2$ and $\psi : E_1 \to E_3$ are nonconstant isogenies. Further assume that φ is separable and $\ker\varphi \subseteq \ker\psi$. Then there exits a unique $\pi : E_2 \to E_3$ such that $\psi = \pi \circ \varphi$.*

7.2 Dual isogenies

In this section we introduce another important object on elliptic curves. The construction of dual isogenies is not that obvious from a geometric point of view. Consider two elliptic curves E_1, E_2 and a nonconstant isogeny (thus surjective) $\varphi : E_1 \to E_2$. Recall that the isogeny induces an homomorphism $\varphi^* : \operatorname{Pic}^0(E_2) \to \operatorname{Pic}^0(E_1)$ defined by

$$[(Q)] \mapsto \left[\sum_{P \in \varphi^{-1}(Q)} e_\varphi(P)(P) \right]$$

where e_φ is φ's ramification index at P. Now if $\kappa_i : E_i \to \operatorname{Pic}^0(E_i)$ be the bijection we constructed in Section 6.2. Then let's investigate the composition $\kappa_1^{-1} \circ \varphi^* \circ \kappa_2$. Take some $Q \in E_2$ and some P such that $\varphi(P) = Q$. Then

$$\begin{aligned}
\left(\kappa_1^{-1} \circ \varphi^* \circ \kappa_2\right)(Q) &= \left(\kappa_1^{-1} \circ \varphi^*\right)[(Q) - (\mathcal{O})] \\
&= \kappa_1^{-1}\left[\sum [e_\varphi(P')(P')] - \sum [e_\varphi(T)(T)]\right] \\
&= \sum_{P' \in \varphi^{-1}(Q)} [e_\varphi(P')]P' - \sum_{T \in \varphi^{-1}(\mathcal{O})} [e_\varphi(T)]T \\
&= [\deg_i \varphi]\left(\sum_{P' \in \varphi^{-1}(Q)} P' - \sum_{T \in \varphi^{-1}(\mathcal{O})} T\right) && \text{by Theorem 7.1.1} \\
&= [\deg_i \varphi \cdot \# \ker \varphi]P \\
&= [\deg_i \varphi \cdot \deg_s \varphi]P = [\deg \varphi]P && \text{by Theorem 7.1.1}
\end{aligned}$$

where the second last equality holds since all $P' \in \varphi^{-1}(Q)$ are of the form $P + T$ for a distinct $T \in \ker \varphi^{-1}(Q)$. However, we do not know if this composition is an isogeny. Therefore, it is reasonable to construct the following object:

Theorem 7.2.1. *Let $\varphi : E_1 \to E_2$ be an isogeny and $\deg \varphi = m$. Then there exists a unique isogeny $\hat{\varphi} : E_2 \to E_1$, called* the dual isogeny of φ, *such that $\hat{\varphi} \circ \varphi = [m]$.*

Proof. We first prove uniqueness. Suppose $\hat{\varphi}, \hat{\varphi}'$ are two dual isogenies, then

$$(\hat{\varphi} - \hat{\varphi}') \circ \varphi = [m] - [m] = [0].$$

This means $\hat{\varphi} - \hat{\varphi}'$ must be a constant, namely $\hat{\varphi} = \hat{\varphi}'$.

To simplify the proof of existence, we use Corollary 5.4.1. Say $\varphi = \psi \circ \varphi_q$ where φ_q is a Frobenius map of degree q and ψ separable. Suppose φ and ψ are two maps of degree m, n respectively whose dual isogenies exist. Then

$$(\hat{\varphi} \circ \hat{\psi}) \circ (\psi \circ \varphi) = \hat{\varphi} \circ [n] \circ \varphi = [n] \circ \hat{\varphi} \circ \varphi = [nm]$$

where the third equality holds since φ is a homomorphism. By uniqueness, $\widehat{\psi \circ \varphi} = \hat{\varphi} \circ \hat{\psi}$. This means if we can prove that the two maps from the Frobenius decomposition have dual isogeny, then the composition of their dual isogeny is the dual isogeny of the original map.

Case 1: φ is separable. Since φ has degree m, we have $\# \ker \varphi = \deg_s \varphi = \deg \varphi = m$. This suggests the extremely crucial conclusion that every element of $\ker \varphi$ has order dividing $[m]$. Thus, $\ker \varphi \subseteq \ker[m]$. By Theorem 7.1.3, there is a unique $\hat{\varphi}$ such that $[m] = \hat{\varphi} \circ \varphi$.

Case 2: φ is the qth power Frobenius map φ_q with $q = p^e$, then $\varphi_q = \varphi_p^e$. Thus it suffices to reduce to the case pth power Frobenius map. We use the fact that if ω is an invariant differential, then $[m]^*\omega = m\omega$, which means $[p]^*\omega = p\omega = 0$. This means the map $[p]$ is not separable, otherwise it violates (iii) in Lemma 5.6.1. Thus we can decompose $[p] = \psi \circ \varphi_p^d$ for some integer $d \geqslant 1$ (otherwise $[p]$ would be separable!). Then taking $\hat{\varphi} = \psi \circ \varphi_p^{d-1}$, one gets the dual isogeny. □

Lemma 7.2.1. *Suppose $\varphi : E_1 \to E_2$ is an isogeny. Then*

(i) $\varphi \circ \hat{\varphi} = [m]$.

(ii) *If $\psi : E_1 \to E_2$ is another isogeny. Then $\widehat{\varphi + \psi} = \hat{\varphi} + \hat{\psi}$.*

(iii) *For all $m \in \mathbb{Z}$, $\widehat{[m]} = [m]$ which suggests* $\deg [m] = m^2$.

(iv) $\deg \hat{\varphi} = \deg \varphi$ *and* $\hat{\hat{\varphi}} = \varphi$.

Proof. (i) We have $(\varphi \circ \hat{\varphi}) \circ \varphi = \varphi \circ [m] = [m] \circ \varphi$. But since φ is nonconstant, $\varphi \circ \hat{\varphi} = [m]$

(ii) The proof of this part is lengthy and difficult, so we omit it.

(iii) Using (ii), $\widehat{[m+1]} = \widehat{[m]} + \widehat{[1]}$. Yet $[0] \circ [0] = [0] = [\deg[0]]$ so $\widehat{[0]} = [0]$, which gives the base case of the induction. Let $d = \deg\, [m]$, then $[d] = [m^2]$, which means $d = m^2$ as $\operatorname{End}(E)$ is torsion-free.

(iv), (v) are easy using (iii). □

Remark 7.2.1. Suppose $\operatorname{char} k = p > 0$. We have collected all necessary properties of the isogeny $[m]$. Thus, we could investigate the structure of $E[m]$, which is the kernel of $[m]$. Taking $n = 0$ in Theorem 7.1.2, if $p \nmid m$, then $[m]$ is separable. Thus, by Theorem 7.1.1, $\#E[m] = \#\ker[m] = \deg\,[m] = m^2$. And since p is prime, for every $d \mid m$, we have $p \nmid d$. Thus, $\#E[d] = d^2$. By looking at the classification of $E[m]$ as a finitely generated group, it must follow that $E[m] \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$.

Now consider the case where $m = p^e$ for some $e \geqslant 1$. Then

$$\#E[p^e] = \#\ker[p^e] = \deg_s[p^e] = (\deg_s(\hat{\varphi}_p \circ \varphi_p))^e$$

But since φ_p, the pth power Frobenius map is purely inseparable by Theorem 5.4.1, the RHS equals $(\deg_s(\hat{\varphi}_p)^e$. If $\hat{\varphi}_p$ is inseparable, then $\#E[p^e] = 1$ which implies $E[p^e] = \{\mathcal{O}\} = 0$. If $\hat{\varphi}_p$ is separable, then $\#E[p^e] = p^e$ and writing out $E[p^e]$'s decomposition as a finite group, we get $E[p^e] \cong \mathbb{Z}/p^e\mathbb{Z}$.

Corollary 7.2.1. *For elliptic curves E_1, E_2, the function*

$$\deg : \mathrm{Hom}(E_1, E_2) \to \mathbb{Z}$$

is a positive definite quadratic form.

Proof. By definition $\deg\varphi = 0$ if and only if $\varphi = [0]$ so it is positive definite. Also, we have $\deg(m\varphi) = \deg[m] \cdot \deg\varphi = m^2 \deg\varphi$ for all $m \in \mathbb{Z}$. So it remains to prove that the polar form of deg:

$$\langle\varphi, \psi\rangle = \deg(\varphi + \psi) - \deg\varphi - \deg\psi$$

is $\mathbb{Z}$-bilinear.

Note the map $[] : \mathbb{Z} \to \mathrm{End}(E_1)$ is an injection, so

$$\begin{aligned}[\langle\varphi, \psi\rangle] &= [\deg(\varphi + \psi)] - [\deg\varphi] - [\deg\psi] \\ &= (\hat{\varphi} + \hat{\psi}) \circ (\varphi + \psi) - \hat{\varphi} \circ \varphi - \hat{\psi} \circ \psi \\ &= \hat{\varphi} \circ \psi + \hat{\psi} \circ \varphi\end{aligned}$$

Since $\hat{\varphi} \circ \psi$ and $\hat{\psi} \circ \varphi$ are both $\mathbb{Z}$-linear (easy to check) in φ and ψ and $[]$ is an injection, the polar form is $\mathbb{Z}$-bilinear. Thus, deg is a positive definite quadratic form. □

7.3 Tate modules

In this section, we get a little bit more "Galois", and see what we can do with the group action $\mathrm{Gal}(K/k)$ on the elliptic curve. Let E be an elliptic curve over K/k. Recall that the explicit formula (Corollary 3.3.1) for $[2]$ shows that if E/k then $[2]$

is also defined over k, meaning for all $\sigma \in \mathrm{Gal}(K/k)$, $[2]^\sigma = [2]$. Thus we know, for any $P \in E$

$$[m]P^\sigma = [m]^\sigma P^\sigma = ([m]P)^\sigma$$

which means $\mathrm{Gal}(K/k)$ acts on each $E[m]$!

Therefore, the group action induces a representation (or in certain texts the group action is itself a representation):

$$\rho : \mathrm{Gal}(K/k) \to \mathrm{Aut}(E[m]) = \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$$

But the ring $\mathbb{Z}/m\mathbb{Z}$ has characteristic > 0, which is hard to work with. Thus, we want some ring of characteristic 0 where the representation would live.

Note that $\mathbb{Z}_l$, the ring of l-adic numbers, is the completion of $\mathbb{Z}_{(p)}$, meaning

$$\mathbb{Z}_l = \varprojlim \mathbb{Z}/l^n\mathbb{Z}$$

where the obvious inverse system is given by maps of the form $\mathbb{Z}/l^{n+m}\mathbb{Z} \xrightarrow{\cdot l^m} \mathbb{Z}/l^n\mathbb{Z}$. Indeed, this ring has characteristic zero, and it relates very closely to the quotients $\mathbb{Z}/l^n\mathbb{Z}$. So it is ideal to make our representations live on this ring. Meanwhile, note that we also have an inverse system of l^n-torsion subgroups of an elliptic curves, namely

$$E[l^{n+m}] \xrightarrow{[l]^m} E[l^n]$$

We can take

Definition 7.3.1. The inverse limit of all l^n-torsion subgroups:

$$T_l(E) = \varprojlim E[l^n]$$

to be the *l-adic Tate module of E.*

Remark 7.3.1. Note that if l is a prime number different from the characteristic of p, then $E[l^n] \cong \mathbb{Z}/l^n\mathbb{Z} \times \mathbb{Z}/l^n\mathbb{Z}$ (Remark 7.2.1), which is a free $\mathbb{Z}/l^n\mathbb{Z}$-module of rank 2. Thus,

$$T_l(E) \cong \mathbb{Z}_l \times \mathbb{Z}_l$$

which is a $\mathbb{Z}_l$-module, with the canonical Krull topology.

Similarly, if $l = p = \mathrm{char}\, k$, then $T_l(E) = 0$ or $\mathbb{Z}_p$.

Remark 7.3.2. The Galois group also acts on $T_l(E)$. To see this, take some element $(,,,,a_2,a_1) \in T_l(E)$. Then we want to show $(...,a_2^\sigma,a_1^\sigma)$ is also in $T_l(E)$ for all $\sigma \in \mathrm{Gal}(K/k)$. This is clear since $a_j = [l]^{j-i}a_i$ suggests

$$a_j^\sigma = ([l]^{j-i}a_i)^\sigma = [l]^{j-1}a_i^\sigma$$

so the property is still preserved.

Thus we have a group representation:

Definition 7.3.2. The representation induced by the group action

$$\rho : \mathrm{Gal}(K/k) \to \mathrm{Aut}(T_l(E))$$

is the *l-adic Galois representation attached to E.*

Remark 7.3.3. For any isogeny $\varphi : E_1 \to E_2$ between elliptic curves (which are homomorphisms so they preserve the torsion subgroups), we have induced maps $\varphi : E_1[l^n] \to E_2[l^n]$ which induce a map

$$\varphi_l : T_l(E_1) \to T_l(E_2)$$

If $E_1 = E_2 = E$, the map $\varphi \mapsto \varphi_l$ is a homomorphism of rings

$$\rho : \mathrm{End}(E) \to \mathrm{End}(T_l(E))$$

The following lemma is an exercise in [Sil09]. We reproduce and solve it here.

Lemma 7.3.1. *The map $\rho : \mathrm{End}(E) \to \mathrm{End}(T_l(E))$ defined by $\varphi \mapsto \varphi_l$ is injective.*

Proof. Suppose $\varphi \in \ker \rho$. Then $\varphi|_{E[l^n]} = 0$ for all n by the construction of φ_l, which means $\#\ker\varphi \geqslant \#E[l^n] = l^{2n}$ for all n. But note that $\#\ker\varphi = \deg_s \varphi$ which is finite if φ is nonconstant. Thus, $\varphi \equiv \mathcal{O}$, suggesting ρ is injective. □

7.4 Weil pairings

Selecting a basis of $E[m]$, which is a $\mathbb{Z}/m\mathbb{Z}$-module, we could define a determinant map $\det : E[m] \times E[m] \to \mathbb{Z}/m\mathbb{Z}$ by selecting a basis $\{T_1, T_2\}$ and letting

$$\det(aT_1 + bT_2, cT_2 + dT_2) = ad - bc.$$

But this determinant might not be Galois invariant. So we define a pairing that's more complicated but nicer.

Take some $T \in E[m]$. Then there is some $f \in K(E)$ such that $\mathrm{div}(f) = m(T) - m(O)$ (since $\kappa([m]T) = m\kappa(T) \equiv \mathcal{O}$ in the Picard group). Take T' such that $[m]T' = T$. Then there is some $g \in K(E)$ such that

$$\mathrm{div}(g) = m^*(T) - m^*(O) = \sum_{R \in E[m]} (T' + R) - (R)$$

It can be checked that $f \circ [m] = g^m$ after multiplying f with a constant. Now fix any $S \in E[m]$. We observe that for all $X \in E$,

$$g(X+S)^m = f([m]X + [m]S) = f([m]X) = g(X)^m$$

which means for each X the function $g(X+S)/g(X)$ only takes finitely many values which are all mth roots of unity. Also, the rational function $\varphi : E \to \mathbb{P}^1$ defined by $S \mapsto [g(X+S)/g(X) : 1]$ is not surjective, meaning it's a constant. Therefore, we can define the pairing

Definition 7.4.1.

$$e_m(S,T) = \frac{g(X+S)}{g(X)}$$

called the *Weil e_m-pairing*.

We will only state the following properties of e_m and will omit the proof as it is superbly lengthy but there is not enough space for it.

Lemma 7.4.1. *The Weil e_m-pairing satisfies:*

(i) *The paring is bilinear: $e_m(S_1 + S_2, T) = e_m(S_1, T)e_m(S_2, T)$ and similarly for the other entry.*

(ii) *The pairing is alternating: $e_m(T,T) = 1$ and thus $e_m(S,T) = e_m(T,S)^{-1}$.*

(iii) *The pairing is Galois invariant: $e_m(S,T)^\sigma = e_m(S^\sigma, T^\sigma)$.*

(iv) *The pairing is nondegenerate: if $e_m(S,T) = 1$ for all $S \in E[m]$ then $T = \mathcal{O}$.*

(v) *For all $S \in E[mm'], T \in E[m]$, $e_{mm'}(S,T) = e_m([m']S, T)$.*

(vi) *There exist $S, T \in E[m]$ such that $e_m(S,T)$ is a primitive mth root of unity, namely if $E[m] \subseteq E(k)$ then $\boldsymbol{\mu}_m \subseteq k^\times$ where $\boldsymbol{\mu}_m$ is the set of mth roots of unity in K.*

(vii) *The adjointness of $\hat{\varphi}$: $e_m(S, \hat{\varphi}(T)) = e_m(\varphi(S), T)$.*

We want to create a pairing on $T_l(E)$ too. This would be a map from $T_l(E) \times T_l(E)$ to $T_l(\boldsymbol{\mu}) = \varinjlim \boldsymbol{\mu}_{l^n}$. Note that the map $\boldsymbol{\mu}_{l^{n+1}} \xrightarrow{z \mapsto z^l} \boldsymbol{\mu}_{l^n}$ form the inverse system of the latter inverse limit. By bilinearity and (v) in Lemma 7.4.1,

$$e_{l^{n+1}}(S,T)^l = e_{l^{n+1}}(S, [l]T) = e_{l^n}([l]S, [l]T)$$

So we have

Definition 7.4.2. The map induced by e_m

$$e : T_l(E) \times T_l(E) \to T_l(\boldsymbol{\mu})$$

is called the *l-adic Weil pairing.*

Remark 7.4.1. Suppose we select a $\mathbb{Z}_l$-basis of $T_l(E)$. Then we can compute the trace and determinant of φ_l for each $\varphi \in \operatorname{End}(E)$. These functions take values in $\mathbb{Z}_l$ and they are independent of the choice of basis.

And finally we use the l-adic Weil pairing to deduce the most important formula in this report:

Theorem 7.4.1. *Let $\varphi \in \operatorname{End}(E)$ and $\varphi_l = \rho(\varphi) \in \operatorname{End}(T_l(E))$. Then*

$$\det(\varphi_l) = \deg \varphi, \quad \operatorname{tr}(\varphi_l) = 1 + \deg \varphi - \deg(1 - \varphi)$$

Proof. The latter formula is immediate from the first formula ($a + d = 1 + ad - bc - (1 - a)(1 - d) + bc$). So it suffices to prove the first formula.

Let $\{v_1, v_2\}$ be a $\mathbb{Z}_l$-basis of $T_l(E)$ and write

$$\varphi_l = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

Then

$$\begin{aligned} e(v_1, v_2)^{\deg \varphi} &= e([\deg \varphi]v_1, v_2) && \text{by bilinearity} \\ &= e(\hat{\varphi}\varphi v_1, v_2) && \text{by construction} \\ &= e(\varphi v_1, \varphi v_2) && \text{by adjointness} \\ &= e(v_1, v_2)^{ad-bc} && \text{by bilinearity and the alternating property} \\ &= e(v_1, v_2)^{\det(\varphi_l)} \end{aligned}$$

and since $e(v_1, v_2)$ is nondegenerate, $e(v_1, v_2) \neq 1$ so $\deg \varphi = \det(\varphi_l)$. □

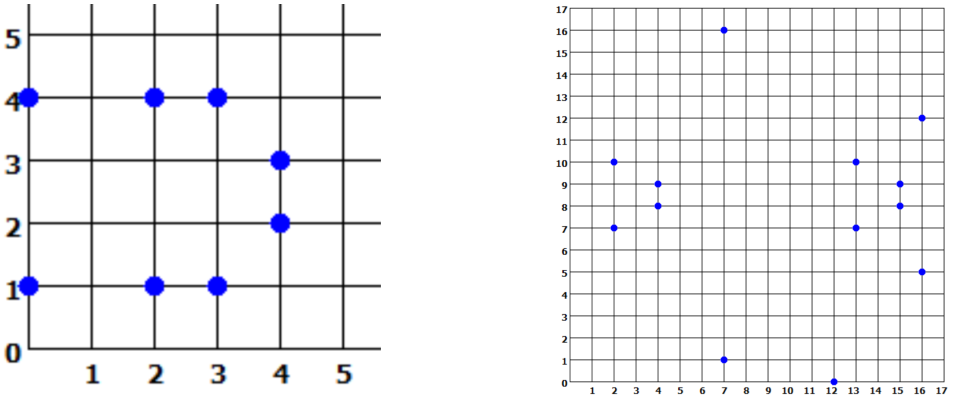
8 Elliptic Curves over Finite Fields

8.1 A bound of the number of rational points

We investigate curves defined on the algebraic closure of a finite fields of size $q = p^r$, where $p \neq 2, 3$ is a prime (note that finite fields are perfect). We consider an example when $q = p = 5$ and the curve $E/\mathbb{F}_5 : y^2 = x^3 + x + 1$. To find rational points on this curve, we just need to substitute x with $0, 1, 2, 3, 4$ into the polynomial $x^3 + x + 1$ and find y to be the square root of the result. In this way, we find 9 points including the point at infinity, namely

$$E(\mathbb{F}_5) = \{O, (0,1), (0,-1), (2,1), (2,-1), (3,1), (3,-1), (4,2), (4,-2)\}.$$

Thus, $E(\mathbb{F}_5)$ is an abelian group of order 9. From the classifications of finitely generated abelian group, we know that $E(F_5)$ is either a product of 2 cyclic groups of order 3 or a cyclic group of order 9. Let $P = (0, 1) \in E(F_5)$. Using the duplication formula, we find that $P = (0, 1), 2P = (4, 2), 3P = (2, 1)$. Thus, the group $E(\mathbb{F}_5)$ is not a product of 2 cyclic groups of order 3 but a cyclic group of order 9. See Figure 3a for a visualization (the point at infinity is not included). Figure 3b is a visualization of rational points in a more complicated case. The visualization tool is obtained from [Tao+12].



(a) $E : y^2 = x^3 + x + 1$ over $\mathbb{F}_5$

(b) $E : y^2 = x^3 + 5x - 3$ over $\mathbb{F}_{17}$

Since there are only q^2 different points in the space $\mathbb{F}_q^2$, so it is clear that the group $E(\mathbb{F}_q)$ is finite and thus finitely generated. But we are still not sure about the size of the set of $E(\mathbb{F}_q)$. In other words, is there an exact formula, or at least an estimate of points in $E(\mathbb{F}_q)$?

Remark 8.1.1. A trivial bound for $\#E(\mathbb{F}_q)$ is $2q+1$ since each x in the Weierstrass equation produces at most two y's plus the additional point at infinity of the curve.

To guess the size of $E(\mathbb{F}_q)$, we first consider some simple cases, namely some curves of low degree. First, we consider the curve of degree 1, which is a line $y = ax + b$. In the Affine plane, we can take any values for x in $\mathbb{F}_q$ and then the value of y is completely determined. And, as for a line, there is always a point at infinity, namely the point $[1, a, 0]$. Thus, there is p+1 points on the line in total. Then, we consider the curve of degree 2, the conic

$$C : ax^2 + bxy + cy^2 + dx + ey + f = 0.$$

It turns out that the set of rational points on the conics whose equations' coefficients are in $\mathbb{F}_q$, $C(\mathbb{F}_q)$, are never empty. So, we can pick a rational point on the conics C as the projective point and then project each point on the conics to a line not passing the projective point by drawing the line passing through the projective point and the point and getting the intersection point of two lines. (we also project the projective point to the line by drawing the tangent line of the conics at the projective point and getting the intersection point of two lines) Thus, we set up a one-to-one correspondence between points on the conics and points on the line. Also, the rational point on the conics are also on-to-one correspondent to the rational points on the lines. So, the number of rational points on a conics is the same as those on a line, which is $(p + 1)$. Now, before returning to our discussion of the curve

$$C : y^2 = f(x),$$

where $f(x)$ is a polynomial with coefficients in $\mathbb{F}(p)$. We substitute different values $x = 0, 1, ..., p - 1$ into $f(x)$, if $f(x) = 0$, then y can only be 0. If $f(x) \neq 0$, then there are two possible y values if $f(x)$ is a square element, and there are no y, if $f(x)$ is a non-square element.That is to say, if $f(x)$ is randomly distributed among the subfield F_q, intuitively speaking, we would expect $q + 1$ points, since each value of x yields either one y, or it has 50% chance of yielding two y's and 50% chance of yielding no y. In fact, Hasse and Weil confirmed this intuitive analysis.

Theorem 8.1.1. *If C is a smooth irreducible curve of genus g defined over a finite field $\mathbb{F}_p$, then the number of $\mathbb{F}_q$-rational points on C is equal to $q + 1 - \epsilon$, where the error term $\epsilon$is not larger than $2g\sqrt{q}$ and $q = p^r$ for some r.*

Corollary 8.1.1. *For all elliptic curves $E/\mathbb{F}_q$,*

$$|\#E(\mathbb{F}_p) - p - 1| \leqslant 2\sqrt{q}$$

Proof. See Section 9.1. □

8.2 Factorization algorithm

The famous cryptosystem RSA involves the problem in number theory called prime factorisation. In this section, the traditional method and the elliptic curve version of prime factorisation algorithms are introduced.

8.2.1 Prime or composite

Fermat's little theorem: if n is prime, then $2^{n-1} \equiv 1 \pmod{n}$. In fact, this works for any integer a not divisible by p. So $a^{n-1} \equiv 1 \pmod{n}$. It is easier to prove Fermat's little theorem using the group $\mathbb{Z}/n\mathbb{Z}$ as one gets the identity raising any element to the $(n-1)$th power. If $2^{n-1} \bmod n \neq 1$, n is composite. Unfortunately, the converse of Fermat's little theorem is not true, so one cannot prove that n is prime in this way.

To determine $a^k \pmod{n}$ where a, k, n are positive integers, write k as a binary number, that is

$$k = \sum_{i=1}^{r} c_i 2^i \quad \text{where } c_i \in \{0, 1\}$$

where $r \leq \log_2 k$. Then $a^k = \prod_{i \text{ s.t. } c_i \neq 0} a^{2^i}$. Define the iterative process

$$A_0 = a, \quad A_{n+1} = A_n^2 \pmod{n}$$

We have $a^k \equiv \prod_{i \text{ s.t. } c_i \neq 0} A_i \pmod{n}$, so it takes at most $2r \leq 2 \log_2 k$ operations (r operations for finding A_i and at most r operations for multiplying all necessary A_i). This is called the fast powering algorithm, with a logarithmic complexity.

8.2.2 Greatest common divisors

The Euclidean algorithm is a quick way to determine $\gcd(a, b)$, letting $a = r_0, b = r_1$, we can apply Euclidean division repeatedly:

$$r_{i-1} = r_i q_i + r_{i+1} \quad \text{where } 0 \leq r_{i+1} < r_i$$

$b = r_1 > r_2 > r_3 > \cdots$ so this process terminates when $r_{n+2} = 0$ and the final equation is $r_n = r_{n+1} q_{n+1}$. It can be proved that $r_{n+1} = \gcd(a, b)$.

Theorem 8.2.1. *The Euclidean algorithm* $O(\log n)$*. The number of steps required for computing* $\gcd(a, b)$ *with Euclidean algorithm is* $\log_2(\max\{2a, 2b\})$*.*

Proof. First note that for all i, $r_{i+1} \leq \frac{1}{2}r_{i-1}$ $(*)$. From the relation $r_{i-1} = r_i q_i + r_{i+1}$ we have

$$r_{i+1} = r_{i-1} - r_i q_i$$

By the decreasing nature of the sequence r_i ($b = r_1 > r_2 > r_3 > \cdots$), there is nothing to prove if $r_i \leq \frac{1}{2}r_{i-1}$. So assume $r_i > \frac{1}{2}r_{i-1}$,

$$r_{i+1} = r_{i-1} - r_i q_i < r_{i-1} - \frac{1}{2}r_{i-1}q_i = r_{i-1}\left(1 - \frac{1}{2}q_i\right)$$

If $q_i = 0$, $r_{i-1} = r_{i+1}$, we get a contradiction. So $q_i \geq 1$ and $r_{i+1} \leq \frac{1}{2}r_{i-1}$. Using $(*)$ one obtains

$$r_{2i} < \frac{1}{2}r_{2(i-1)} < \cdots < \frac{1}{2^{i-1}}r_1 = \frac{1}{2^{i-1}}b$$

If $2^{i-1} \geq b$ $(**)$, then $r_{2i} < 1$, the only such nonnegative integer is 0. $(**)$ happens when $i \geq 1 + \log_2 b = \log_2(2b)$. So the Euclidean algorithm terminates after $2\log_2(2b)$ steps. But one may begin with $b = r_0, a = r_1$ instead, so we take the maximum of $2a, 2b$. □

The prime factorization of small a, b is a feasible plan, but may not be efficient for larger numbers.

8.2.3 Pollard's $p - 1$ algorithm

For small number n, one can find its prime factorization by listing all primes smaller than $\sqrt{n}$ and pull out factors by brute-force. The time complexity grows exponentially with n so this is not a wise algorithm for larger numbers.

Suppose $n = pq$ where p is prime, by Fermat's little theorem, $a^{p-1} \equiv 1 \pmod{p}$ if a is coprime to p. So $a^{m(p-1)} \equiv 1 \pmod{p}$ for any positive integer m. Namely, given $k = m(p-1)$, $a^k - 1 = pr$ for some integer r. Clearly $p|\gcd(pr, pq) = \gcd(a^{m(p-1)} - 1, n)$. But without knowing any factor in the beginning, we can only take a try when k is a product of small primes. Usually a is chosen to be 2, but choosing any small prime that does not divide n suffices.

Then using the fast powering algorithm and the Euclid algorithm, one can compute $a^k - 1 \pmod{n}$ and $e = \gcd(a^k - 1, n)$ within $2\log_2(2kn)$ operations ($2\log_2(k)$ for fast powering and $2\log_2(2n)$ for Euclidean algorithm). If n do have a prime factor p with $p - 1|k$, then $p|a^k - 1$, and $e \geq p > 1$. So the following outcomes require a different approach:

- $e = 1$: this k fails (no prime factor p s.t. $p - 1|k$) and we need to increase k

- $e = n$: this is a trivial factor and we have to change choice of a
- $1 < e < n$, we have a factor of n, and we can write n as a product of two smaller numbers. Although e may not be prime, we can repeat the process on $e, n/e$ and even further until we get prime factors.

The number k can be chosen to be $d!$ ($d = 2, 3, \cdots$). As d increases, we must eventually meet a prime factor p of n s.t. $p|d!$, so $\gcd(a^k - 1, n) > 1$ and process terminates (unless $\gcd(a^k - 1, n) = n$, but this has an extremely low probability for large n). So the algorithm is only efficient if there is a prime factor s.t. $p - 1$ is product of small primes to small powers.

Definition 8.2.1 (B-power smooth)**.** A number is called B-power smooth if and only if given its prime factorization $\prod_{i=1}^{r} p_i^{e_i}$, for each i, $p_i^{e_i} \leq B$.

So Pollard's $p - 1$ algorithm works well with B-power smooth numbers when B is a relatively small number. This yields another way to pick k:

$$k = \prod_{\substack{p \text{ prime} \\ 1 \leq p \leq B}} p^{\left\lfloor \frac{\log B}{\log p} \right\rfloor}$$

where B is chosen around 10^5 to 10^6, and it is increased when $e = 1$.

If all $(\mathbb{Z}/p\mathbb{Z})^\times$ (p is prime factor of n) have orders divisible by a large prime p_l, for most choices of a, $e = 1$ for k until k increases to a value such that $p_l|k$.

Example 8.2.1. Let $n = 1329 = 347 \times 383$. $347 - 1 = 2 \times 173$, $383 - 1 = 2 \times 191$ ($173, 191$ are all primes). Let $p_1 = 347, p_2 = 383$. So as element of $(\mathbb{Z}/p_i\mathbb{Z}, +)$, except $a \equiv 0, \pm 1 \mod p_i$, any other a has order $p_i/2$ or p_i. That means unless it happens that $(p_1/2)|k$ or $(p_2/2)|k$, otherwise, for most a, $\gcd(a^k - 1, n) = 1$. $p - 1$ being divisible by large prime is not rare, out of 16 primes between 300 and 400, there are 3 primes p ($347, 359, 383$) s.t. $p - 1$ has a prime factor larger than 100.

This makes Pollard's algorithm on $(\mathbb{Z}/p\mathbb{Z})^\times$ very risky. Lenstra suggested to use the group $E(\mathbb{F}_p)$ instead. Then not only we can choose k, but also the curve E. By Theorem 9.1.1,

$$|E(\mathbb{F}_p)| = p + 1 - \epsilon_p \quad \text{where } |\epsilon_p| \leq 2\sqrt{p}$$

and Birch [Bir68] showed that among the finite choices of curve E over finite field, ϵ_p is spread out between $\pm 2\sqrt{p}$. So the problem of large prime dividing some $p - 1$ ($p|n$) can be solved by trying many curves E.

The process itself is almost a copy of Pollard $p-1$ algorithm on $\mathbb{Z}/p\mathbb{Z}$, if $|E(\mathbb{F}_p)|| k$, then $[k]P = \mathcal{O}$ in $E(\mathbb{F}_p)$. While calculating $[k]P$, we have a chance of getting a factor of n. But there are some technical details:

- **Requirements on** n We need $\gcd(n, 6) = 1$ so that $E(\mathbb{F}_3), E(\mathbb{F}_2)$ will not be involved. Because transformation into Weierstrass normal form requires $\text{char}(F_p) = p \neq 3$ and removing quadratic term for cubic of x in the form requires $p \neq 2$. Also we require n not to be a perfect power (checked by finding $n^{\frac{1}{m}}$ for $m \in \mathbb{N}$ until getting an integer or $n^{\frac{1}{m}} < 2$. In the latter case, n is not a perfect power). The third requirement is that n should be odd; otherwise, keep taking out factor 2 until it becomes odd.

- **Choice of elliptic curve** The Weierstrass normal form without the quadratic term in x is
$$y^2 \equiv x^3 + bx + c \pmod{n}$$
One can choose the curve (i.e. choose b, c randomly) first and suffer to find solution x, y to this modulus equation, or one can save time by randomly choosing b, x_1, y_1 and let $c \equiv y_1^2 - x_1^3 - bx_1 \pmod{n}$. We define the point $P = (x_1, y_1)$ and it is on the curve.

- **Computation of** $[k]P$ Just like fast powering algorithm, calculating $[k]P$ by first finding $P_r = [2^r]P$ with iterations is faster. Thus we add all the P_i required to get $[k]P$. But we should work on mod n not on $\mathbb{Q}$ as the coordinates may blow up. So the duplication formulas may fail: the tangent at $Q = (x, y)$
$$\lambda = \frac{f'(x)}{2y} \equiv \frac{2x^2 + 2ax + b}{2y} \pmod{n}$$
either $\gcd(2y, n) = 1$ (i.e. $\gcd(y, n) = 1$ as n is odd) or $\gcd(2y, n) > 1$. In the first case, $2y$ has an inverse so we are able to double Q. In the second case, if $\gcd(y, n) < n$, we have a nontrivial factor of n. But if $\gcd(y, n) = n$, we have to change k or the curve E. Similarly when adding two points A, B, $\frac{y_B - y_A}{x_B - x_A}$ may not always be defined and when $1 < \gcd(x_B - x_A, n) < n$, we get a nontrivial factor of n.

A figure of full steps of Lenstra's algorithm is given below Note in this algorithm,

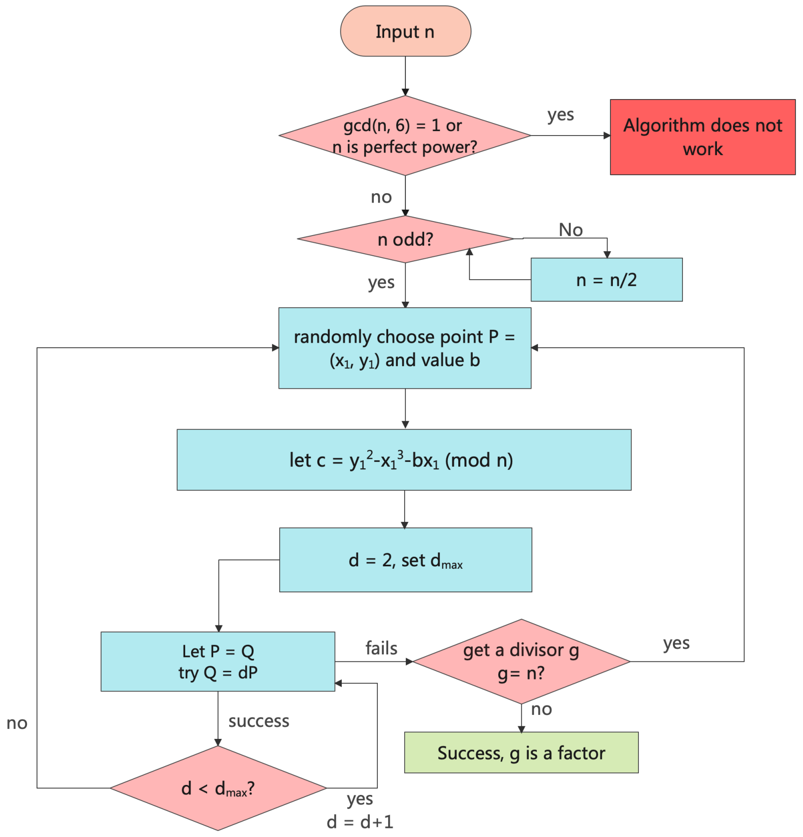


Figure 4: Flow chart of Lenstra's idea

the value of $[k]P$ does not really matter, the factor is obtained when calculation of $[k]P$ fails. This is the funny part, you can only succeed (get a factor of n) if you fail.

Efficiency: Just like Pollard's $p-1$ algorithm, the algorithm works well if $|E(\mathbb{F}_p)|$ is B-smooth. If E is randomly chosen, this has probability u^{-u} where $u = \frac{\ln p}{\ln B}$. And using this probability, estimate the complexity of Lenstra's algorithm is $O(e^{E\sqrt{r \log r}})$ where r is the number of bits in n and E is the smallest number s.t. $(d_{\max})!$ is E-smooth.

8.3 Cryptography

A cryptosystem consists of a function f that can encipher (or encrypt), a message m, and $e = f(m)$ is sent to the receiver. In *classical cryptosystem* (or private key cryptosystem), f is kept secret (more precisely, the parameters of f, also called *encipher key*, are kept secret). With the encipher key, one can easily find a *decipher key* to decipher the message by applying f^{-1} to e. For example, if $f(m) = m + 2 \mod n$, then encipher key is 2 and decipher key is -2, then $f^{-1}(e) = e - 2 \mod n$. But without the key, it should be difficult to find f^{-1}. So two parties must meet once to exchange the keys before communicating online safely.

However, for security concerns, two parties using a classical cryptosystem usually update the keys frequently to avoid being cracked. But frequent exchanges of keys (in person, or via a trusted third party) is very inconvenient. So *public key cryptosystems* are created, which can potentially solve this. Encipher keys are no longer kept private, but f is changed to a *trapdoor* function (such function is difficult to invert. Ideally, the decryption complexity without a decryption key should be polynomial-time, and the complexity with the key should be logarithmic). Only with the help of a specific decipher key, one can invert the function and decode the encrypted message. Key steps

1. Find some decipher key, for example, some large numbers. Use them to construct a trapdoor function f.
2. Publish f (or the encipher keys) so that everyone who wants to send message to you can encrypt the message
3. After receiving the message, use decipher key to decode.

There is no need for two parties to meet in person. The disadvantage if public-key cryptosystem is that decrypting or encrypting takes longer and the capacity of the message is small. So a public key cryptosystem is always used to exchange keys for the private key cryptosystem, and the latter is used for main communications.

8.3.1 RSA

The RSA is a public-key cryptosystem, we will skip the process of encoding a string message like “elliptic” to a number. Assume the information being exchanged is just a number P, here are the steps for constructing the RSA

- Choose two large primes randomly p, q (not too close) and let $N = pq$.

- Choose a random integer e s.t. $\gcd(e, \phi(N)) = 1$ where $\phi(N)$ is the number of integers between $1, N$ that is coprime to N and for $N = pq$, $\phi(N) = (p-1)(q-1)$.
- With p, q, it is easy to find $d = e^{-1} \pmod{\phi(N)}$. The number d is the decipher key for our algorithm
- Publish N, e (encipher keys) but conceal d, p, q.
- Encryption: $f(P) = P^e \text{ (mod } N)$, decryption: $f^{-1}(C) = C^d \text{ (mod } N)$

Two functions in the last step are indeed the inverse of each other

$$f^{-1}(f(P)) = P^{de} \text{ (mod } N) = P \text{ (mod } N)$$

as d, e are the inverse of each other in $\mathbb{Z}/N\mathbb{Z}$. It is believed that without p, q, one cannot find d easily. And two powerful methods for factorization (in order to compute p, q) are the elliptic curve factorization (described in the previous section) and the number field sieve:

- Number field sieve takes approximately $e^{c\sqrt[3]{\log N}}$ of time where c is some small constant. And numbers considered impossible to be factored are $N \geq 2^{2048} \approx 10^{617}$. It works faster than the elliptic curve factorization if $p \approx q$.
- If $p \ll q$, the elliptic curve method takes about $e^{c\sqrt{\log p}}$, and it is faster than the number field sieve. Yet, the number of bits required for N to be infeasible to decompose is huge.

While the difficulty of factorizing large primes is the foundation of RSA, the difficulty for finding m s.t. $a^m \equiv b \text{(mod } p)$ allows us to build a trapdoor function for *discrete logarithm problem*(DLP).

When studying prime factorization, we changed the scope from the group $(\mathbb{Z}/p\mathbb{Z})^\times$ to $C(\mathbb{F}_p)$ which improved efficiency. Similarly, DLP can be used on any group. With group $G = C(\mathbb{F}_p)$, we get *elliptic curve discrete logarithm problem* (ECDLP) where given $P, Q \in C(\mathbb{F}_p)$, it is believed that finding m s.t. $[m]P = Q$ is difficult (the idea of introducing elliptic curves to DLP is provided by Neal Koblitz and Victor Miller in mid-1980s).

The ECDLP may be harder to crack compared to DLP because the powerful tool to solve DLP, index calculus, relies on the fact that $\mathbb{Q}^\times_{\{}(p)\} := \{a/b \in \mathbb{Q} : p \nmid b\}^\times$ is infinitely generated by "small" generators. But by Mordell's theorem, $C(\mathbb{Q})$ is finitely generated, so the index calculus fails. For ECDLP, any $p > 2^{200}$ is considered secure instead of requiring $p > 2^{2048}$.

Cryptography is a field that still lacks theoretical support, for example, it is hard to prove if a trapdoor function is really difficult to invert, or maybe such an inversion algorithm is not yet invented. The complexity of an algorithm also requires rigorous proof. And there are various schemes of cryptosystems, each with its own strength (more efficient than others in some cases).

9 The p-Riemann Hypothesis

The prominent and difficult Riemann Hypothesis was first presented by Riemann himself in 1859 [Rie59], concerning the real part of the nontrivial zeros of the analytic continuation of the zeta function

$$\zeta(s) = \sum_{n\geqslant 1} \frac{1}{n^s}$$

The mathematical genius Euler proved that

$$\zeta(s) = \prod_{p \text{ prime}} \frac{1}{1-p^{-s}}$$

in 1740.

While people had no idea about how one might prove or disprove the Riemann Hypothesis, Emil Artin studied a generalized version of this zeta function. Let R be an algebra of finite type over $\mathbb{Z}$ (we don't care what this means). Then for any maximal ideal ideal $\mathfrak{m} \lhd R$, the residue field $R/\mathfrak{m}$ is finite. Artin then defined a generalized zeta function by

$$\zeta_R(s) = \prod_{\mathfrak{m} \text{ maximal}} \frac{1}{1-\#(R/\mathfrak{m})^{-s}}$$

Note that if $R = \mathbb{Z}$ then the maximal ideals are of the form $p\mathbb{Z}$ and then $\zeta_{\mathbb{Z}}(s)$ is just the regular Riemann zeta function. Unfortunately this definition did not provide the mathematicians with anything special or useful for Riemann Hypothesis [Oor14]. In his Ph.D. thesis, Emil Artin presented an analogous definition of the zeta function $Z(V;T)$ on algebraic curves V over finite fields [Art24]. This zeta function is also called the Hasse–Weil zeta function. This new zeta function then proved to be fruitful, and led to some fruitful developments in geometry and number theory.

With this new zeta function on algebraic curves over a finite field $\mathbb{F}_q$ of characteristic $p > 0$, German mathematicians were able to produce a similar version of Riemann Hypothesis, called the *p-Riemann Hypothesis*, on the properties of $Z(V;T)$. The zeta function $Z(V;T)$ is essentially a generating function of the sizes of the sets $V(\mathbb{F}_{q^n})$ representing the $\mathbb{F}_{q^n}$-rational points in V.

9.1 The Hasse bound

Suppose $E/\mathbb{F}_q$ is an elliptic curve and q is a power of some prime p. As mentioned in Section 8.1, one might be interested in bounding the number of $\mathbb{F}_q$-rational points in E. Corollary 8.1.1 was conjectured by Artin in his Ph.D. thesis, and proven by Hasse latter in 1930s.

Theorem 9.1.1 (Hasse bound)**.** *Let $E/\mathbb{F}_q$. Then*

$$|\#E(\mathbb{F}_q) - q - 1| \leqslant 2\sqrt{q}$$

Proof. Let $\varphi_q : E \to E$ be the qth Frobenius map. Since the Galois group $\mathrm{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q)$ is topologically generated by the Frobenius endomorphism $F : x \mapsto x^q$ (that the cyclic group $\langle F\rangle$ is dense in $\mathrm{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q)$ with respect to its Krull topology).; equivalently, the restriction of every $\sigma \in \mathrm{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q)$ to $\mathbb{F}_{q^n}$ is a power of F. Thus,

$$P \in E(\mathbb{F}_q) = E^{\mathrm{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q)} \text{ if and only if } \varphi_q(P) = \varphi$$

which means $E(\mathbb{F}_q) = \ker(1 - \varphi_q)$. By Theorem 7.1.2 and Theorem 7.1.1, $\#E(\mathbb{F}_q) = \deg(1 - \varphi_q)$. Since $\deg[1] = 1^2 = 1$ and $\deg \varphi_q = q$, by Corollary 7.2.1 and Lemma 1.2.1,

$$|\#E(\mathbb{F}_q) - q - 1| = |\deg(1 - \varphi_q) - \deg[1] - \deg \varphi_q| \leqslant 2\sqrt{\deg[1] \cdot \deg \varphi_q} = 2\sqrt{q}$$

which completes the proof. □

Example 9.1.1. Let $f(x) = ax^3 + bx^2 + cx + d$ be a cubic with distinct roots in $\mathbb{F}_q[x]$. Let $\chi : \mathbb{F}_q^\times \to \{\pm 1\}$ be the character which determines if an element is a square in $\mathbb{F}_q$. One immediately sees that the number of solutions to $E : y^2 = f(x)$ is (with the point at infinity)

$$\#E(\mathbb{F}_q) = 1 + \sum_{x \in \mathbb{F}_q} [1 + \chi(f(x))] = 1 + q + \sum_{x \in \mathbb{F}_q} \chi(f(x))$$

which suggests

$$\left|\sum_{x\in\mathbb{F}_q}\chi\left(f(x)\right)\right|\leqslant 2\sqrt{q}$$

by Theorem 9.1.1.

9.2 Weil conjectures

The Weil conjectures consist of several conjectures concerning the properties of the zeta function defined on algebraic varieties (which was primarily defined by Emil Artin in his Ph.D. thesis, mentioned in section 0). Given a smooth projective variety $V/\mathbb{F}_q$, we define similarly the set of $\mathbb{F}_{q^r}$-rational points on V, denoted by $N_r = \#V(\mathbb{F}_{q^r})$.

Definition 9.2.1. The *zeta function of* $V/\mathbb{F}_q$ is the power series

$$Z(V/\mathbb{F}_q;T)=\exp\left(\sum_{r=1}^{\infty}\frac{N_r}{r}T^r\right)$$

where the exponential of a power series with no constant term is defined by

$$\exp(F(T))=\sum_{k=0}^{\infty}\frac{F(T)^k}{k!}$$

Remark 9.2.1. If we know the zeta function, we could recover each N_r from it:

$$N_r=\frac{1}{(r-1)!}\,\frac{d^r}{dT^r}\log Z(V/\mathbb{F}_q;T)\bigg|_{T=0}$$

Example 9.2.1. Let's try an easy example. Consider the projective space $V=\mathbb{P}^n$. Then the number of points in $V(\mathbb{F}_{q^r})$ is simply $N_r=\frac{q^{r(n+1)-1}}{q^r-1}=\sum_{i=0}^{n}q^{ir}$ (discard the zero tuple and dividing out the equivalence classes). Thus, we have

$$\log Z(V/\mathbb{F}_q;T)=\sum_{r=1}^{\infty}\sum_{i=0}^{n}\frac{(q^iT)^r}{n}=\sum_{i=0}^{n}-\log(1-q^iT)$$

where the second equality holds by exchanging the summation. Thus,

$$Z(V/\mathbb{F}_q;T)=\frac{1}{(1-T)\cdots(1-q^nT)}$$

Remark 9.2.2. What is the set $E(\mathbb{F}_{q^n})$ essentially? Similar to what was argued in Theorem 9.1.1, $E(\mathbb{F}_{q^n})$ is the set of fixed points of the nth iterate of the qth power Frobenius map φ_q. Therefore, we have $\#E(\mathbb{F}_{q^n}) = \ker(1-\varphi_q^n)$, which opens a path way to proving a particular case of the Weil conjectures Hasse used in 1936 [Has36].

The history of the Weil conjectures is also quite interesting. Hasse solved the p-Riemann Hypothesis for curves of genus one, i.e., elliptic curves, and proved Theorem 9.1.1. Weil was aware of this result, and announced an outline of the proof for curves of genus g (Theorem 8.1.1) in 1940, when he was a prisoner "in a French military prison for failing to report for duty" [Bae19]! In 1941 Weil published a proof of Theorem 8.1.1. Weil then studied equations of the form

$$a_0x_0^{m_0} + \cdots + a_rx_r^{m_r} = b$$

over some finite fields, and when $b = 0$, Weil found that

$$\sum_{n=1}^{\infty} N_nT^{n-1} = \frac{d}{dT}\log\left(\frac{1}{(1-T)\cdots(1-q^rT)}\right) + (-1)^r\frac{d}{dT}\log P(T)$$

for some polynomial P [Mil16]. Weil then wrote, in [Wei49], that his observation of the homogeneous equations over finite fields might lead to some "conjectural statements", which are rephrased and restate below. These famous statements are the so-called "Weil conjectures". A brief remark on the name of the last statement is in Remark 9.3.1.

Theorem 9.2.1 (Weil conjectures)**.** *Let $V/\mathbb{F}_q$ be a smooth projective variety of dimension N. Then*

(i) *Rationality: $Z(V/\mathbb{F}_q;T) \in \mathbb{Q}(T)$.*

(ii) *Functional equation: there is an integer ε — the Euler characteristic of V — such that $Z(V/\mathbb{F}_q;1/q^NT) = \pm q^{N\varepsilon/2}T^{\varepsilon}Z(V/\mathbb{F}_q;T)$.*

(iii) *p-Riemann Hypothesis:*

$$Z(V/\mathbb{F}_q;T) = \frac{P_1(T)P_3(T)\cdots P_{2N-1}(T)}{P_0(T)P_2(T)\cdots P_{2N}(T)}$$

where $P_i \in \mathbb{Z}[T]$, $P_0(T) = 1-T$ and $P_{2N} = 1-q^NT$. Furthermore, each P_i factors over $\mathbb{C}$ with roots α_{ij} satisfying $|\alpha_{ij}| = q^{1/2}$ for all i, j. The degree of P_i, b_i, is the ith Betti number *of V.*

As noted before, a baby version of these "conjectures" was proved by Hasse in 1930s. In 1950s, Weil proved these statements for abelian varieties — varieties with an abelian structures but, unlike elliptic curves, are of arbitrary genus and dimension. Grothendieck proved the first two statements for general projective varieties using his theory of étale cohomology, but was unable to prove the p-Riemann Hypothesis. In 1973, Deligne presented his first proof of Weil conjectures [Del74]; in 1980, Deligne presented another proof [Del80]. Deligne's proof was described by Gowers as a "surprise" from Weil's belief of the need of "standard conjectures". Deligne took a "different route", in spite of using Grothendieck's cohomology theory [Gow13].

9.3 Hasse's proof for elliptic curves

Due to the extreme difficulty of the Weil conjectures for general varieties and the level of knowledge required to understand them, we only present the proof of Weil conjectures for elliptic curves — smooth projective varieties of genus one and dimension one. This proof is due to Hasse and was done years before Weil conjectures.

Lemma 9.3.1. *Let $E/\mathbb{F}_q$ be an elliptic curve. Let φ_q be the qth power Frobenius map and suppose*

$$a = q + 1 - \#E(\mathbb{F}_q)$$

Then

(i) *Let $\alpha, \beta \in \mathbb{C}$ be roots of $T^2 - aT + q$. Then $\beta = \bar{\alpha}$ and $|l\alpha| = |\beta| = \sqrt{q}$ and for all $n \geqslant 1$,*

$$N_n = \#E(\mathbb{F}_{q^n}) = q^n + 1 - \alpha^n - \beta^n$$

(ii) *The characteristic polynomial of φ is $T^2 - aT + q$.*

Proof. By Theorem 7.1.2, $1 - \varphi_q$ is separable and by Theorem 7.1.1,

$$\#E(\mathbb{F}_q) = \#\ker(1 - \varphi_q) = \deg(1 - \varphi_q)$$

By Theorem 7.4.1, for any prime $l \neq p$

$$\det(\varphi_{q,l}) = \deg \varphi_q = q, \quad \operatorname{tr}(\varphi_{q,l}) = 1 + \deg \varphi_q - \deg(1 - \varphi_q) = 1 + q - \#E(\mathbb{F}_q) = a$$

Thus by the degree-trace formula, $\varphi_{p,l}$ has characteristic polynomial $\det(T - \varphi_{p,l}) = T^2 - aT + q$, which factors over $\mathbb{C}$ as $(T - \alpha)(T - \beta)$.

(i) Since for all $m/n \in \mathbb{Q}$, if $T = m/n$ then by Theorem 7.4.1,

$$\det(T - \varphi_{p,l}) = \frac{\det(m - n\varphi_{p,l})}{n^2} = \frac{\deg(m - n\varphi_{p,l})}{n^2} \geqslant 0,$$

the quadratic function is also nonnegative for all reals. Thus, the roots must be the same or they must be two complex conjugates. In either case, we have $|\alpha| = |\beta|$. But since $\alpha\beta = \det(\varphi_{p,l}) = q$, we get $|\alpha| = |\beta| = \sqrt{q}$.

Similarly, $E(\mathbb{F}_{q^n})$ is the fixed field of φ_q^n. Then as $\varphi_{p,l}$ is equivalent to $\operatorname{diag}(\alpha, \beta)$ or $J_2(\alpha)$, the Jordan canonical normal form of $\varphi_{p,l}^n$ is always $\operatorname{diag}(\alpha^n, \beta^n)$ or $J_2(\alpha^n)$. Thus,

$$\#E(\mathbb{F}_{q^n}) = \deg(1 - \varphi_q^n) = \det(1 - \varphi_{q,l}^n) = 1 - \alpha^n + \beta^n + q^n$$

(ii) We have by Cayley–Hamilton,

$$\deg(\varphi_q^2 - a\varphi_q + q) = \det(\varphi_{q,l}^2 - a\varphi_{q,l} + q) = 0$$

which by the positive definiteness of the quadratic form deg, $\varphi_q^2 - a\varphi_q + q$=0. □

Theorem 9.3.1 (Weil conjectures for elliptic curves)**.** *Let $E/\mathbb{F}_q$ be an elliptic curve. Then there is an $a \in \mathbb{Z}$ such that*

$$Z(E/\mathbb{F}_q; T) = \frac{1 - aT + qT^2}{(1 - T)(1 - qT)}$$

and (the Euler characteristic is zero; which is already known since $2 - 2g = 0$)

$$Z(E/\mathbb{F}_q; 1/qT) = Z(E/\mathbb{F}_q; T)$$

and finally

$$1 - aT + qT^2 = (1 - \alpha T)(1 - \beta T), \quad |\alpha| = |\beta| = \sqrt{q}$$

Proof. With all our works, the proof is surprisingly easy.

$$\begin{aligned} \log Z(E/\mathbb{F}_q; T) &= \sum_{n=1}^{\infty} \frac{N_n T^n}{n} && \text{by definition} \\ &= \sum_{n=1}^{\infty} \frac{(1 - \alpha^n - \beta^n + q^n)T^n}{n} && \text{by Lemma 9.3.1} \\ &= -\log(1 - T) + \log(1 - \alpha T) \\ &\quad + \log(1 - \beta T) - \log(1 - qT) \end{aligned}$$

Thus,

$$Z(E/\mathbb{F}_q; T) = \frac{(1 - \alpha T)(1 - \beta T)}{(1 - T)(1 - qT)}$$

and the other results are then obvious. □

Remark 9.3.1. Define a function $\zeta_{E/\mathbb{F}_q}(s)$ on $\mathbb{C}$ to be

$$\zeta_{E/\mathbb{F}_q}(s) = Z(E/\mathbb{F}_q; q^{-s}) = \frac{1 - aq^{-s} + q^{1-s}}{(1-q^{-s})(1-q^{1-s})}$$

Then we have $\zeta_{E/\mathbb{F}_q}(s) = \zeta_{E/\mathbb{F}_q}(1-s)$, which is derived from the functional equation. Furthermore, $\zeta_{E/\mathbb{F}_q}(s) = 0$ if and only if $q^{-s} = \alpha$ or β. This means $|q^s| = q^{\mathrm{Re}(s)} = \sqrt{q}$ or $\mathrm{Re}(s) = \frac{1}{2}$. This why the last statement is called the p-Riemann Hypothesis!

10 References

[AM94] M.F. Atiyah and I.G. MacDonald. *Introduction To Commutative Algebra*. Addison-Wesley series in mathematics. Avalon Publishing, 1994. ISBN: 9780813345444. URL: https://books.google.co.uk/books?id=HOASFid4x18C.

[Art24] E. Artin. "Quadratische Körper im Gebiete der höheren Kongruenzen. I." In: *Mathematische Zeitschrift* 19.1 (Dec. 1924), pp. 153–206. ISSN: 1432-1823. DOI: 10.1007/BF01181074. URL: https://doi.org/10.1007/BF01181074.

[Art71] Emil Artin. *Galois Theory: Lectures Delivered at the University of Notre Dame*. Vol. 2. University of Notre Dame, 1971. URL: https://projecteuclid.org/ebooks/notre-dame-mathematical-lectures/Galois-Theory/toc/ndml/1175197041 (visited on 06/20/2022).

[Bae19] John Baez. *The Riemann Hypothesis (Part 3)*. The n-Category Café, 2019. URL: https://golem.ph.utexas.edu/category/2019/09/the_riemann_hypothesis_part_3.html (visited on 06/20/2022).

[Bir68] B. J. Birch. "How the Number of Points of An Elliptic Curve Over a Fixed Prime Field Varies". In: *Journal of the London Mathematical Society* s1-43.1 (1968), pp. 57–60. DOI: https://doi.org/10.1112/jlms/s1-43.1.57. eprint: https://londmathsoc.onlinelibrary.wiley.com/doi/pdf/10.1112/jlms/s1-43.1.57. URL: https://londmathsoc.onlinelibrary.wiley.com/doi/abs/10.1112/jlms/s1-43.1.57.

[Cha05] Anne-Sophie Charest. *Pollard's p-1 and Lenstra's Factoring Algorithms*. 2005. URL: https://www.math.mcgill.ca/darmon/courses/05-06/usra/charest.pdf (visited on 06/20/2022).

[Con16] Conifold. *Who first identified the group structure of an elliptic curve?* History of Science and Mathematics Stack Exchange, 2016. URL: https://hsm.stackexchange.com/questions/5171/who-first-identified-the-group-structure-of-an-elliptic-curve (visited on 06/20/2022).

[Del74] Pierre Deligne. "La conjecture de Weil : I". fr. In: *Publications Mathématiques de l'IHÉS* 43 (1974), pp. 273–307. URL: http://www.numdam.org/item/PMIHES_1974__43__273_0/.

[Del80] Pierre Deligne. "La conjecture de Weil : II". fr. In: *Publications Mathématiques de l'IHÉS* 52 (1980), pp. 137–252. URL: http://www.numdam.org/item/PMIHES_1980__52__137_0/.

[Ful89] William Fulton. *Algebraic Curves: an introduction to algebraic geometry.* Addison-Wesley, 1989.

[Gow13] W. T. Gowers. *The Work of Pierre Deligne*. 2013. URL: https://gowers.files.wordpress.com/2013/03/peterd.pdf.

[Har10] Robin Hartshorne. *Algebraic Geometry*. Springer, 2010.

[Has36] Helmut Hasse. "Zur Theorie der abstrakten elliptischen Funktionenkörper III. Die Struktur des Meromorphismenrings. Die Riemannsche Vermutung." In: *Journal für die reine und angewandte Mathematik* 175 (1936), pp. 193–208. URL: http://eudml.org/doc/149968.

[Jue96] C. Juel. "Ueber die Parameterbestimmung von Punkten auf Curven zweiter und dritter Ordnung. Eine geometrische Einleitung in die Theorie der logarithmischen und elliptischen Functionen". In: *Mathematische Annalen* 47 (1896), pp. 72–104. URL: http://eudml.org/doc/157783.

[Kob12] Neal Koblitz. *A Course in Number Theory and Cryptography.* Vol. 192-198. Springer, 2012.

[Mil16] J. S. Milne. "The Riemann Hypothesis over Finite Fields: From Weil to the Present Day". In: ed. by Lizhen Ji, Frans Oort, and Shing-Tung Yau. The Legacy of Bernhard Riemann after One Hundred and Fifty Years. International Press of Boston, Inc., 2016, pp. 487–566.

[Mor22] L. J. Mordell. "On the rational solutions of the indeterminate equations of the third and fourth degrees." English. In: *Proc. Camb. Philos. Soc.* 21 (1922), pp. 179–192. ISSN: 0008-1981.

[Oor14] Frans Oort. "Wei Conjectures". In: *Nieuw Archief Voor Wiskunde* 1 (2014), p. 211. URL: http://www.nieuwarchief.nl/serie5/pdf/naw5-2014-15-3-211.pdf (visited on 06/20/2022).

[Poo99] Bjorn Poonen. "An explicit algebraic family of genus-one curves violating the Hasse principle". In: (1999). DOI: 10.48550/ARXIV.MATH/9910124. URL: https://arxiv.org/abs/math/9910124.

[Rei88] Miles Reid. *Undergraduate Algebraic Geometry.* Cambridge University Press, 1988.

[Rie59] Bernard Riemann. "Ueber die Anzahl der Primzahlen unter einer gegebenen Grösse". In: *Monatsberichte der Königlich Preußischen Akademie der Wissenschaften zu Berlin* (1859).

[Sil09] Joseph H Silverman. *The Arithmetic of Elliptic Curves*. Springer-Verlag, 2009.

[SS97] S. Stevenhagen and B. de Smit. *Kernvak Algebra*. 1997. URL: https://websites.math.leidenuniv.nl/algebra/ellcurves.pdf (visited on 06/20/2022).

[ST15] Joseph H Silverman and John Tate. *Rational points on Elliptic Curves*. Springer, 2015.

[Tao+12] Jun Tao et al. "ECvisual: A Visualization Tool for Elliptic Curve Based Ciphers". In: *Proceedings of the 43rd ACM Technical Symposium on Computer Science Education*. SIGCSE '12. Raleigh, North Carolina, USA: Association for Computing Machinery, 2012, pp. 571–576. ISBN: 9781450310987. DOI: 10.1145/2157136.2157298. URL: https://doi.org/10.1145/2157136.2157298.

[Vak17] Ravi Vakil. *The Rising Sea: foundations of Algebraic Geometry*. 2017. URL: http://math.stanford.edu/~vakil/216blog/FOAGnov1817public.pdf (visited on 06/20/2022).

[Wei49] André Weil. "Numbers of Solutions of Equations in Finite Fields". In: *Bulletin of the American Mathematical Society* 55 (1949), pp. 497–508. DOI: 10.1090/s0002-9904-1949-09219-4. (Visited on 06/20/2022).

[Wik22] Wikipedia contributors. *Torus — Wikipedia, The Free Encyclopedia*. https://en.wikipedia.org/w/index.php?title=Torus&oldid=1082687949. [Online; accessed 22-June-2022]. 2022.