A Brief Introduction to Elliptic Curves and Modular Curves

Hongxiang Zhao

December 1, 2022

Abstract

This is a note about elliptic curves and modular curves on a seminar about modular forms. Thus, we assume some basic properties about the Weierstrass $\wp$-functions and j-functions. We aim not to depend on much knowledge from algebraic geometry and Riemann surfaces. Further topics about elliptic curves and modular curves may be found in [12] and [8].

Contents

1 From Ellipses to Elliptic Curves

1.1 Elliptic Functions

Given an ellipse $\frac{x^2}{a^2} + \frac{y^2}{b^2} = 1$ with $a \geqslant b > 0$. We want to know the arc length of it. Setting $x = a\sin t, y = b\cos t, k = \frac{\sqrt{a^2-b^2}}{a}$, we get the arc length of the ellipse:

$$L = 4a\int_0^{\frac{\pi}{2}} \sqrt{1 - k^2\sin^2 t}dt \tag{1}$$

Now set $u = \sin t$. Then (1) becomes

$$L = 4a\int_0^1 \frac{1-k^2u^2}{\sqrt{(1-u^2)(1-k^2u^2)}}du$$

which cannot be evaluated in terms of elementary functions. Legendre studied integrals of the form $\int R(t)/\sqrt{P(t)}dt$, where R is a rational function and P is a polynomial of degree 4, which is now called the elliptic integral. He showed that the integral can be reduced to three integrals:

$$\int_0^\Phi \frac{du}{\sqrt{(1-u^2)(1-k^2u^2)}} \quad \int_0^\Phi \frac{u^2du}{\sqrt{(1-u^2)(1-k^2u^2)}} \quad \int_0^\Phi \frac{du}{(1+nu^2)\sqrt{(1-u^2)(1-k^2u^2)}}$$

where $0 \leqslant \Phi \leqslant 1$ [10]. Note that when $k = 0$, the first integral is the case of circle and becomes the inverse of the sine function. Observing that, Abel suggested that the inverse of such integral may be more convenient to use, which we now call elliptic functions. Following Abel's idea, Jacobi found that the inverse of the first integral is doubly periodic after extended to $\mathbb{C}$, which is similar to sine function with one period 2π. Moreover, the only meromorphic single-valued functions with two periods are elliptic functions [10]. Thus, we have the following definition:

Definition 1.1 (Elliptic Functions)**.** Let $\Lambda \subset \mathbb{C}$ be a lattice, that is, a discrete subgroup of $\mathbb{C}$ that contains a $\mathbb{R}$-basis for $\mathbb{C}$. An **elliptic function** (relative to the lattice Λ) is a meromorphic function $f(z)$ on $\mathbb{C}$ that satisfies $f(z+\omega) = f(z)$ for all $z \in \mathbb{C}$ and all $\omega \in \Lambda$.

The set of all such functions is denoted by $\mathbb{C}(\Lambda)$. It is clear that $\mathbb{C}(\Lambda)$ is a field.

Now we need some properties of elliptic functions for further uses.

Definition 1.2. The **fundamental parallelogram** for Λ is a set of the form

$$D = \{a + t_1\omega_1 + t_2\omega_2 : 0 \leqslant t_1, t_2 < 1\}$$

where $a \in \mathbb{C}$ and $\{\omega_1, \omega_2\}$ is a basis for Λ. It is clear that the natural map $D \to \mathbb{C}/\Lambda$ is bijective.

Theorem 1.3. *Let $f \in \mathbb{C}(\Lambda)$ be an elliptic function relative to a lattice Λ. Let D be a fundamental parallelogram for Λ such that f has no zeros or poles on ∂D. Then*

(a) $\sum_{\omega \in D} res_\omega(f) = 0$.

(b) $\sum_{\omega \in D} ord_\omega(f) = 0$.

(c) $\sum_{\omega \in D} ord_\omega(f)\omega \in \Lambda$.

Proof. (a) By the residue theorem and the periodicity of f, we have

$$\sum_{\omega \in D} \text{res}_\omega(f) = \frac{1}{2\pi i} \int_{\partial D} f(z) dz = 0$$

(b) Since f is periodic, f' is also periodic. By the argument principle,

$$\sum_{\omega \in D} \text{ord}_\omega(f) = \int_{\partial D} \frac{f'(z)}{f(z)} dz = \sum_{\omega \in D} \text{res}_\omega(f'/f) = 0$$

(c) By residue theorem,

$$\begin{aligned} \sum_{\omega \in D} \text{ord}_\omega(f)\omega &= \frac{1}{2\pi i} \int_{\partial D} \frac{z f'(z)}{f(z)} dz \\ &= \frac{1}{2\pi i} \left(\int_a^{a+\omega_1} + \int_{a+\omega_1}^{a+\omega_1+\omega_2} + \int_{a+\omega_1+\omega_2}^{a+\omega_2} + \int_{a+\omega_2}^{a} \right) \frac{z f'(z)}{f(z)} dz \end{aligned}$$

By change of variable and the periodicity of f,

$$\sum_{\omega \in D} \text{ord}_\omega(f)\omega = -\frac{\omega_2}{2\pi i} \int_a^{a+\omega_1} \frac{f'(z)}{f(z)} dz + \frac{\omega_1}{2\pi i} \int_a^{a+\omega_2} \frac{f'(z)}{f(z)} dz$$

Note that for any meromorphic function $g(z)$ with $g(a) = g(b)$, $\frac{1}{2\pi i} \int_a^b \frac{g'(z)}{g(z)} dz$ is the winding number around 0 of the path

$$[0,1] \to \mathbb{C}, \quad t \mapsto g\big((1-t)a + tb\big)$$

which is an integer. Thus, $\sum_{\omega \in D} \text{ord}_\omega(f)\omega \in \Lambda$.

□

1.2 Weierstrass Equations

Given a lattice Λ on $\mathbb{C}$, we have the Weierstrass $\wp$-function and the Eisenstein series

$$\wp(z;\Lambda) := \frac{1}{z^2} + \sum_{\substack{\omega\in\Lambda\\ \omega\neq 0}} \left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right)$$

$$G_{2k}(\Lambda) := \sum_{\substack{\omega\in\Lambda\\ \omega\neq 0}} \omega^{-2k}$$

We know that the Weierstrass $\wp$-function satisfies the ODE:

$$\big(\wp'(z)\big)^2 = 4\wp(z)^3 - g_2\wp(z) - g_3$$

where $g_2 = g_2(\Lambda) = 60G_4(\Lambda)$ and $g_3 = g_3(\Lambda) = 140G_6(\Lambda)$. Thus, given any $z \in \mathbb{C}\setminus\Lambda$, we get a corresponding point on the curve $y^2 = 4x^3 - g_2x - g_3$ by setting $(x,y) = \big(\wp(z), \wp'(z)\big)$. If $z = 0$, since the order of pole of $\wp'(z)$ at $z = 0$ is greater than $\wp(z)$, this induces a map

$$\begin{aligned} \phi\colon \mathbb{C}/\Lambda &\to E(\mathbb{C}) \\ z &\to [\wp(z), \wp'(z), 1],\ z \neq 0 \\ 0 &\mapsto [0,1,0] \end{aligned} \tag{2}$$

where $E(\mathbb{C})$ is a projective curve in $\mathbb{P}^2(\mathbb{C})$ defined by $y^2z = 4x^3 - g_2xz^2 - g_3z^3$. See [12, Proposition VI.3.6]

Remark. *Actually there is a heuristic way to get such ODE by viewing $\wp$ as the inverse of an elliptic integral. Extend $I(\Phi) = \int_O^\Phi \frac{du}{\sqrt{(1-u^2)(1-k^2u^2)}}$ to complex numbers and temporarily ignore that the square root is not well-defined on the whole complex plane. Let*

$$v^2 = (1-u^2)(1-k^2u^2) = k^2(u-\alpha)(u-\beta)(u-\gamma)(u-\delta)$$

and $x = \frac{1}{u-\alpha}, y = \frac{v}{(u-\alpha)^2}$. Then we have $y^2 = s(x^3 + ax^2 + bx + c)$ for some $s, a, b, c \in \mathbb{C}$ and

$$J(\Phi) := -I(\frac{1}{\Phi} + \alpha) = \int_{-\frac{1}{\alpha}}^{\Phi} \frac{dx}{\sqrt{x^3 + ax^2 + bx + c}}$$

Recall that $\wp$ is originated from the inverse of such integral. In fact, it is the inverse of $J(\Phi) =$

$\int_O^\Phi \frac{dx}{\sqrt{f(x)}}$ *according to [1], where* $f(x) = x^3 - g_2x - g_3$. *Since* $\wp \circ I(\Phi) = \Phi$,

$$\wp'\big(I(\Phi)\big) = \sqrt{f(\Phi)} = \sqrt{f\Big(\wp\big(I(\Phi)\big)\Big)}$$

Denoting $z = I(\Phi)$ *we get the ODE.*

To generalize the equation given in the previous subsection to arbitrary field K, we consider a projective curve in $\mathbb{P}^2$ over K given by an equation of the form:

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3$$

Here $O = [0, 1, 0]$ is the base point and $a_1, \cdots, a_6 \in \bar{K}$. Such an equation is called a **Weierstrass equation**. Let $x = X/Z, y = Y/Z$. We get a curve

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

with a point $O = [0, 1, 0]$ at infinity. If $a_1, \cdots, a_6 \in K$, then E is said to be defined over K.

Definition 1.4 (Elliptic Curves)**.** An **elliptic curve** E is a smooth projective curve in $\mathbb{P}^2$ given by a Weierstrass equation with a based point $O = [0, 1, 0]$.

By a projective curve we mean a projective (irreducible) variety of dimension 1 (equivalently, the coordinate ring has Krull dimension 1).

By smooth projective we mean that for curve C given by $V(f_1, \cdots, f_r)$ in $\mathbb{P}^n$, the matrix $\left(\frac{\partial f_i}{\partial x_j}(P)\right)$ has dimension $n - 1$ for every $P \in C$.

If $\mathrm{char}(K) \neq 2$, then we can make a coordinate change $y \mapsto \frac{1}{2}(y - a_1x - a_3)$. Then the equation becomes the form satisfied by Weierstrass $\wp$-function:

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

where $b_2 = a_1^2 + 4a_2, b_4 = 2a_4 + a_1a_3, b_6 = a_3^2 + 4a_6$.

Definition 1.5. The discriminant, the j-invariant and the invariant differential associated to the

given Weierstrass equation are defined as:

$$\Delta := -b_2^2(b_2b_6 - b_4^2) - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6$$
$$j := (b_2^2 - 24b_4)^3/\Delta$$

Note that when $b_2 = 0, b_4 = -\frac{1}{2}g_2, b_6 = -g_3$, $\Delta = g_2^3 - 27g_3^2$ and $j = \frac{(12g_2)^3}{\Delta}$ are in accord with the ones given by modular forms. Then we have the following statements similar to the case when $K = \mathbb{C}$.

Proposition 1.6. *(a) Two elliptic curves are isomorphic over $\bar{K}$ if and only if they have the same j-invariant.*

(b) If $j_0 \in \bar{K}$, then there exists an elliptic curve defined over $K(j_0)$ whose j-invariant is equal to j_0.

Proof. See [12, Proposition III.1.4]. □

2 Group Laws on Elliptic Curves

Since we have a bijection $\phi\colon \mathbb{C}/\Lambda \to E(\mathbb{C})$ and $\mathbb{C}/\Lambda$ is a compact Lie group, we can give an abelian group structure on $E(\mathbb{C})$ via ϕ. Actually this group operation admits a geometry meaning on elliptic curves:

Theorem 2.1 (Bézout's Theorem)**.** *Let C, C' be two distinct curves in $\mathbb{P}^2$ with degree m, n respectively. Assume that C, C' have no common component. Then C intersects C' at exactly mn points, counting with multiplicity.*

Given points P, Q on an elliptic curve E, let L be the line connecting P, Q (if $P = Q$, then let L to be the tangent line, the tangent line at O is $Z = 0$). By Bézout's theorem, L intersects E at another point R. Let L' be the line connecting R, O. Then define the addition of P, Q to be the third point of $E \cap L'$.

Proposition 2.2. *The operation defined above makes E an abelian group with the identity O.*

Proof. The only non-trivial part is the associativity. For the proof of the associativity, one way is to deduce the explicit formula of the addition and then verify by direct calculation. For the explicit formula, see [12, Section III.2]. The second way is to prove that the elliptic curve is

isomorphic to its Picard group as sets by $P \mapsto (P) - (O)$ and satisfying $(P + Q) + (O) = (P) + (Q)$ in the Picard group. Then we can conclude by the associativity of the Picard group. For details, see [12, Proposition III.3.4]. The method we use here is a more geometric one. We first need a lemma in algebraic geometry.

Lemma 2.3. *Let C be an irreducible cubic smooth curve in $\mathbb{P}^2$. Let C', C'' be two cubic curves in $\mathbb{P}^2$. Suppose $C' \cap C$ and $C'' \cap C$ agree on eight points. Then they will agree on the remaining point.*

Proof. See [4, Chapter 5, Proposition 3]. □

Suppose $P, Q, R \in E$. Suppose L_1 is the line connecting P, Q and intersecting with E at another point S', M_1 is the line connecting S, S', O, L_2 is the line connecting S, R and intersecting with E at another point T. Then $T = (P + Q) + R$.

On the other hand, suppose M_2 is the line connecting Q, R and intersecting with E at another point U', L_3 is the line connecting $U, U\prime, O$, M_3 is the line connecting P, U and intersecting with E at another point T'. Then $T' = P + (Q + R)$.

Let $C' = L_1L_2L_3$ and $C'' = M_1M_2M_3$, where $L_1L_2L_3, M_1M_2, M_3$ denotes the curve given by the multiplication of the formulas of the three lines. Then we conclude by the lemma above. □

Remark. *In history, the group law rises independently on the correspondence of tori and elliptic curves. It is discovered by Newton during his investigation of cubic curves [10]. So it is kind of surprising that these two groups are isomorphic.*

Definition 2.4 (Isogeny)**.** For two elliptic curves E_1, E_2, isogenies are nonconstant group homomorphisms between E_1, E_2.

Theorem 2.5. *The map*

$$\begin{aligned} \phi\colon \mathbb{C}/\Lambda &\to E(\mathbb{C}) \\ z &\to [\wp(z), \wp'(z), 1],\ z \neq 0 \\ 0 &\mapsto [0, 1, 0] \end{aligned} \tag{3}$$

is a group isomorphism.

Proof. Pick any $z_1, z_2 \in \mathbb{C}/\Lambda$.

If z_1 or z_2 is 0 in $\mathbb{C}/\Lambda$, the case is trivial since $[0, 1, 0]$ is the identity element in $E(\mathbb{C})$.

If $z_1, z_2 \neq 0$ and $z_1 + z_2 = 0$, note that the line connecting $[x_0 : y_0 : 1]$ and $[0 : 1 : 0]$ in $\mathbb{P}^2$ is $x - x_0 z = 0$, intersecting with E at $[x_0 : -y_0 : 1]$, so in $E(\mathbb{C})$

$$\begin{aligned}[\wp(z_1) : \wp'(z_1) : 1] + [\wp(z_2) : \wp'(z_2) : 1] &= [\wp(z_1) : \wp'(z_1) : 1] + [\wp(z_1) : -\wp'(z_1) : 1] \\ &= [0 : 1 : 0] = \phi(z_1 + z_2)\end{aligned}$$

If $z_1, z_2 \neq 0$ and $z_1 + z_2 \neq 0$, we are going to show that in $E(\mathbb{C})$,

$$[\wp(z_1) : \wp'(z_1) : 1] + [\wp(z_2) : \wp'(z_2) : 1] = [\wp(z_1 + z_2) : \wp'(z_1 + z_2) : 1]$$

Thus, we are going to prove that $\big(\wp(z_1), \wp'(z_1)\big), \big(\wp(z_2), \wp'(z_2)\big), \big(\wp(-z_1 - z_2), \wp'(-z_1 - z_2)\big)$ lie on a line in $\mathbb{C}^2$. Let $ax + by + c$ be the line in $\mathbb{C}^2$ connecting $\big(\wp(z_1), \wp'(z_1)\big), \big(\wp(z_2), \wp'(z_2)\big)$. If $z_1 \neq z_2$, the elliptic function $f = a\wp(z) + b\wp'(z) + c$ has two distinct zeros z_1, z_2. Since f is dominant by $\wp'$, f has three poles in some fundamental parallelogram. By Theorem 1.3(b), f has three zeros in the same fundamental parallelogram. By Theorem 1.3(c), the third zero of f is $-z_1 - z_2$ modulo Λ. If $z_1 = z_2$, we need to show that f has a double zero on z_1. Suppose the three zeros of f are z_1, z_3, z_4. Since $z_1 + z_2 \neq 0$, $b \neq 0$. Since $ax + by + c$ is the tangent line at $\wp(z_1), \wp(z_1)$ is at least a double zero of $4x^3 + g_2 x + g_3 - (\frac{ax+c}{b})^2 = 4(x - x_1)(x - x_2)(x - x_3)$. We may assume that $x_1 = x_2 = \wp(z_1)$. Then z_1 is at least a double zero of the elliptic function $4(\wp(z) - \wp(z_1))^2(\wp(z) - x_3)$. Note that the six zeros of $4(\wp(z) - \wp(z_1))^2(\wp(z) - x_3)$ are $\pm z_1, \pm z_3, \pm z_4$. Since $z_1 \neq -z_1$, we may assume $z_1 = \pm z_3$. If $z_1 = -z_3$, $\wp'(z_1) = 0$. Let $\omega_3 = \omega_1 + \omega_2$. Then for each i,

$$\wp'\left(\frac{\omega_i}{2}\right) = \wp'\left(-\frac{\omega_i}{2}\right) = -\wp'\left(\frac{\omega_i}{2}\right)$$

Note that $\wp(z) - \wp(\omega_i/2)$ is an elliptic curve with double zero on $\omega_i/2$, so $\omega_1/2, \omega_2/2, \omega_3/2$ are distinct in $\mathbb{C}/\Lambda$. Thus, $\omega_1/2, \omega_2/2, \omega_3/2$ are the three zeros of $\wp'$, contradicting to $2z_1 \neq 0$ in $\mathbb{C}/\lambda$, so $z_1 = z_3$. □

3 Elliptic Curves over $\mathbb{C}$

3.1 Complex Multiplication

In fact, there are bijections of morphisms between tori, lattices and elliptic curves.

Theorem 3.1. *Let Λ_1, Λ_2 be two lattices in $\mathbb{C}$ and suppose $\alpha \in \mathbb{C}$ such that $\alpha\Lambda_1 \subset \Lambda_2$. Then scalar multiplication by α induces a well-defined holomorphic homomorphism $\psi_\alpha \colon \mathbb{C}/\Lambda_1 \to \mathbb{C}/\Lambda_2$ given by $\psi_\alpha(z) = \alpha z \pmod{\Lambda_2}$. Then we have*

(a) The map $\{\alpha \in \mathbb{C} : \alpha\Lambda_1 \subset \Lambda_2\} \to \{$holomorphic $\psi \colon \mathbb{C}/\Lambda_1 \to \mathbb{C}/\Lambda_2$ with $\psi(0) = 0\}$ given by $\alpha \mapsto \psi_\alpha$ is a bijection.

(b) Let E_1, E_2 be elliptic curves associated to lattices Λ_1, Λ_2 respectively. Then the map $\{$isogenies $\psi \colon E_1 \to E_2\} \to \{$holomorphic $\psi \colon \mathbb{C}/\Lambda_1 \to \mathbb{C}/\Lambda_2$ with $\psi(0) = 0\}$ given by $\psi \mapsto \phi_2^{-1} \circ \psi \circ \phi_1$ is a bijection, where ϕ_1, ϕ_2 are maps given in 2 corresponding to Λ_1, Λ_2 respectively.

Proof. See [12, Theorem III.4.1]. The proof depends on some properties of Riemann surfaces, $\wp$-fucntions and isogenies not mentioned in this note. □

Definition 3.2 (Order)**.** Let L be a number field, i.e. a finite extension over $\mathbb{Q}$. An **order** $\mathcal{O}$ of L is a subring of L that is a finitely generated abelian group and satisfies $\mathcal{O} \otimes \mathbb{Q} = L$.

Theorem 3.3. *Let $E/\mathbb{C}$ be an elliptic curve, and let ω_1, ω_2 be generators for the lattice Λ associated to E. Then one of the following is true:*

(i) End$(E) = \mathbb{Z}$.

(ii) The field $\mathbb{Q}(\omega_1/\omega_2)$ is an imaginary quadratic extension of $\mathbb{Q}$, and End(E) is isomorphic to an order in $\mathbb{Q}(\omega_1/\omega_2)$.

Proof. Let $\mathcal{O} = \{\alpha \in \mathbb{C} \colon \alpha\Lambda \subset \Lambda\}$. By Theorem 3.1, we know that $\mathrm{End}(E) = \mathcal{O}$. Let $\tau = \frac{\omega_1}{\omega_2}$. Since Λ is homothetic to $\mathbb{Z} + \mathbb{Z}\tau$, we may assume that $\Lambda = \mathbb{Z} + \mathbb{Z}\tau$. For any $\alpha \in \mathcal{O}$, we have

$$\alpha = a + b\tau \qquad \alpha\tau = c + d\tau$$

for some $a, b, c, d \in \mathbb{Z}$, so $\mathbb{Z} \subset \mathcal{O} \subset \mathbb{Z} + \mathbb{Z}\tau \subset \mathbb{Q}(\tau)$. Thus, $\mathcal{O}$ is a finitely generated abelian group.

If $\mathcal{O} \neq \mathbb{Z}$, pick $\alpha \in \mathcal{O} - \mathbb{Z}$, then $b \neq 0$. By eliminating α, we get

$$b\tau^2 + (a - d)\tau - c = 0$$

Since $\tau \notin \mathbb{R}$, $\mathbb{Q}(\tau)/\mathbb{Q}$ is an imaginary quadratic extension. Since $b\tau \in \mathcal{O}$, $\mathcal{O} \otimes \mathbb{Q} = \mathbb{Q}(\tau)$. Therefore, $\mathcal{O}$ is an order in $\mathbb{Q}(\tau)$. □

Definition 3.4 (Complex Multiplication)**.** Let E/K be an elliptic curve. Then we say that E has **complex multiplication** if $\mathrm{End}(E) \neq \mathbb{Z}$.

3.2 The Inverse Map from Elliptic Curve to Tori

In this section we discuss the inverse map of 2. This section may be skipped due to time limit.

Since we are discussing curves over an algebraic field $\mathbb{C}$, the right-hand side of Weierstrass equations can be factored into linear terms.

Definition 3.5 (Legendre Form)**.** A Weierstrass equation is in the **Legendre form** if it can be written as

$$y^2 = x(x-1)(x-\lambda)$$

Proposition 3.6. *Suppose that char$(K) \neq 2$. Then every elliptic curve is isomorphic over $\bar{K}$ to an elliptic curve in Legendre form*

$$E_\lambda : y^2 = x(x-1)(x-\lambda)$$

for some $\lambda \in \bar{K}$ with $\lambda \neq 0, 1$.

Proof. Suppose that an elliptic curve E is given by

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

Replacing y by $2y$ and factoring the right-hand side, we get

$$E : y^2 = (x-e_1)(x-e_2)(x-e_3)$$

for some $e_1, e_2, e_3 \in \bar{K}$. Since $\Delta = 16(e_1-e_2)^2(e_1-e_3)^2(e_2-e_3)^2 \neq 0$, e_1, e_2, e_3 are distinct. Now we substitute $x = (e_2-e_1)x' + e_1$ and $y = (e_2-e_1)^{\frac{3}{2}}y'$, we get

$$(e_2-e_1)^3(y')^2 = (e_2-e_1)^3x'(x'-1)(x'-\lambda)$$
$$(y')^2 = x'(x'-1)(x'-\lambda)$$

which is the desired Legendre form with $\lambda = \frac{e_3-e_1}{e_2-e_1} \in \bar{K}$ and $\lambda \neq 0, 1$. □

Now we can give the inverse function of ϕ in 2. Heuristically, recall $\wp\colon \mathbb{C} \to \mathbb{P}^1$ is defined as the inverse function of an elliptic integral, which is $\int_0^z \frac{dx}{\sqrt{4x^3-g_2x-g_3}}$. However, the square root is not well-defined on the whole $\mathbb{P}^1$ space. Thus, we have to make branch cuts on it. By making some coordinate changes, we may assume that an elliptic curve is given in Legendre form $y^2 = x(x-1)(x-\lambda)$ and the Weierstrass $\wp$-function is the inverse function of $\int_0^z \frac{dx}{\sqrt{x(x-1)(x-\lambda)}}$ with $\lambda \notin \mathbb{R}_{\leqslant 0}$. Let

$$B := (\mathbb{R}_{\leqslant 0} \cup \infty) \cup L$$

where L is the straight line connecting $1, \lambda$ in $\mathbb{C}$. Then $\sqrt{x}, \sqrt{\frac{x-1}{x-\lambda}}$ are well-defined on $\mathbb{P}^1 \setminus B$. Thus, $\sqrt{x(x-1)(x-\lambda)}$ is well-defined on $\mathbb{P}^1 \setminus B$. Hence, we obtain a map $\mathbb{P}^1 \setminus B \to \mathbb{C}$. Note that there is a projection $\pi\colon E(\mathbb{C}) \to \mathbb{P}^1$ given by $(x, y) \to x$, which is a double cover ramifying at $0, 1, \lambda, \infty$. Thus, we get a composition

$$E(\mathbb{C}) \setminus \pi^{-1}(B) \xrightarrow{\pi} \mathbb{P}^1 \setminus B \xrightarrow{\text{“}\wp^{-1}\text{”}} \mathbb{C} \longrightarrow \mathbb{C}/\Lambda$$

$$(x, y) \longmapsto x \longmapsto \int_0^x \frac{d\tilde{x}}{\sqrt{\tilde{x}(\tilde{x}-1)(\tilde{x}-\lambda)}} \longmapsto [\int_0^x \frac{d\tilde{x}}{\sqrt{\tilde{x}(\tilde{x}-1)(\tilde{x}-\lambda)}}]$$

Note that $E(\mathbb{C}) \setminus \pi^{-1}(B) \cong (\mathbb{P}^1 \setminus B) \sqcup (\mathbb{P}^1 \setminus B)$ and $y^2 = x(x-1)(x-\lambda)$ on $E(\mathbb{C})$. Thus, we can lift the path integral from 0 to x in $\mathbb{P}^1 \setminus B$ to a path O to $P = (x, y)$. Now we see that it is natural to consider the map $E(\mathbb{C}) \to \mathbb{C}/\Lambda$ given by $P \mapsto \int_O^P \frac{dx}{y}$, and it turns out to be the desired inverse of ϕ in 2.

Proposition 3.7. *Let $E/\mathbb{C}$ be an elliptic curve with Weierstrass coordinate functions x, y.*

(a) Let α, β be closed paths on $E(\mathbb{C})$ giving a basis for $H_1(E; \mathbb{Z})$. Then the periods

$$\omega_1 = \int_\alpha \frac{dx}{y} \qquad \omega_2 = \int_\beta \frac{dx}{y}$$

are $\mathbb{R}$-linearly independent.

(b) Let Λ be the lattice generated by ω_1, ω_2. Then the map $\psi\colon E(\mathbb{C}) \to \mathbb{C}/\Lambda$ given by $P \mapsto \int_O^P \frac{dx}{y}$ is a complex analytic isomorphism of Lie groups. It is the inverse of the map ϕ given in 2.

Proof. (a) By surjectivity of the j-function there is a lattice Λ and a map $\phi\colon \mathbb{C}/\Lambda \to E(\mathbb{C})$ given by $z \mapsto [\wp(z), \wp'(z), 1]$, which is an analytic isomorphism of compact Lie groups. Pulling back α, β, we have $\omega_1 = \int_{\phi^{-1}\circ\alpha} \frac{d\phi^*(x)}{\phi^*(y)} = \int_{\phi^{-1}\circ\alpha} dz$ and similarly $\omega_2 = \int_{\phi^{-1}\circ\beta} dz$.

Since α, β are basis of $H_1(E;\mathbb{Z})$, $\phi^{-1}\circ\alpha, \phi^{-1}\circ\beta$ are basis of $H_1(\mathbb{C}/\Lambda;\mathbb{Z})$. Note that $H_1(\mathbb{C}/\Lambda;\mathbb{Z})$ is naturally isomorphic to Λ via the map $\gamma \to \int_\gamma dz$. Thus, ω_1, ω_2 is a basis of Λ, which is $\mathbb{R}$-linearly independent.

(b) Since $F^*(dz) = d(z\circ F) = \frac{dx}{y}$ and $\phi^{-1}\left(\frac{dx}{y}\right) = dz$, $(F\circ\phi)^*(dz) = dz$. Since $F\circ\phi$ is an endomorphism of $\mathbb{C}/\Lambda$, $F\circ\phi = \psi_\alpha$ for some $\alpha \in \mathbb{C}^*$ by Theorem 3.1. Thus, $dz = (F\circ\phi)^*(dz) = \alpha dz$ implies that $\alpha = 1$. Thus, $F = \phi^{-1}$.

□

4 Modular Curves

Let $\mathscr{R}$ denotes the set of all lattices in $\mathbb{C}$. By Theorem 3.1, two elliptic curves are isomorphic if and only if the corresponding lattices are homothetic. We know that $\mathscr{R}/\mathbb{C}^* \cong \mathbb{H}/\mathrm{SL}_2(\mathbb{Z})$ by [11, Chapter VII, Section 2, Proposition 3]. Therefore, this induces a bijection:

$$\begin{aligned}\{\text{isomorphism classes of elliptic curves } E/\mathbb{C}\} &\to \mathbb{H}/\mathrm{SL}_2(\mathbb{Z}) \cong \mathbb{C}\\ E \cong \mathbb{C}/\Lambda(1,\tau) &\mapsto \quad [\tau] \quad \mapsto j(\tau)\end{aligned}$$

The last isomorphism is by [11, Chapter VII, Section 3, Proposition 5]We have a similar description for general congruence subgroups of $\mathrm{SL}_2(\mathbb{Z})$.

4.1 Congruence Subgroups

Definition 4.1 (Congruence Subgroup)**.** For each integer $N \geqslant 1$, define

$$\begin{aligned}\Gamma(N) &= \ker\Big(\mathrm{SL}_2(\mathbb{Z}) \to \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})\Big)\\ &= \left\{\begin{pmatrix}a & b\\ c & d\end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})\colon b\equiv c\equiv 0 \pmod N \text{ and } a\equiv d\equiv 1 \pmod N\right\}\end{aligned}$$

A **congruence subgroup** of $\mathrm{SL}_2(\mathbb{Z})$ is a subgroup $\Gamma < \mathrm{SL}_2(\mathbb{Z})$ such that $\Gamma \supset \Gamma(N)$ for some $N \geqslant 1$. It follows that the following two subgroups are congruence subgroups.

$$\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \colon c \equiv 0 \pmod{N} \right\}$$

$$\Gamma_1(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \colon c \equiv 0 \pmod{N} \text{ and } a \equiv d \equiv 1 \pmod{N} \right\}$$

In case of $\Gamma = \mathrm{SL}_2(\mathbb{Z})$, we just say that $\mathbb{H}^*/\mathrm{SL}_2(\mathbb{Z}) = \mathbb{H}/\mathrm{SL}_2(\mathbb{Z}) \cup \{\infty\}$. This is because $\mathrm{SL}_2(\mathbb{Z})$ acts transitively on $\mathbb{P}^1(\mathbb{Q}) = \mathbb{Q} \cup \infty$. For a general congruence subgroup Γ, Γ may not act transitively on $\mathbb{P}^1(\mathbb{Q})$. Therefore, we should define $\mathbb{H}^* = \mathbb{H} \cup \mathbb{P}^1(\mathbb{Q})$.

The images of $\mathbb{P}^1(\mathbb{Q})$ under the projection $\mathbb{H}^*/\Gamma$ are called the **cusps** of Γ. This is because that if $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ takes ∞ to a rational number x, $\gamma(D)$ is a region with cusp x, where D is the fundamental domain of $\mathrm{SL}_2(\mathbb{Z})$.

Then we can generalize the definition of modular functions for $\mathrm{SL}_2(\mathbb{Z})$ to modular functions for Γ.

Definition 4.2. Let Γ be a level N congruence subgroup of $\mathrm{SL}_2(\mathbb{Z})$, i.e. N is the least number such that $\Gamma(N) \subset \Gamma$. A meromorphic function f on $\mathbb{H}$ is called a **modular function of weight** k **for** Γ if it satisfies

(a) $f(z) = (cz + d)^{-k} f(\gamma z)$ for all $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma$.

(b) f is meromorphic at each cusp of $\mathbb{H}^*/\Gamma$.

The condition (b) means the following: for each cusp x, there is a $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$, such that $\gamma(\infty) = x$. Let $(f|_k\gamma)(z) := (cz + d)^{-k} f(\gamma z)$, so that the behavior of f near x is relevant to the behavior of $f|_k\gamma$ near ∞. In fact $(f|_k\gamma)$ is invariant under $\sigma = \begin{pmatrix} 1 & N \\ 0 & 1 \end{pmatrix}$ by direct calculation. Then $f|_k\gamma$ admits a Fourier expansion

$$(f|_k\gamma)(q_N) = \sum a_\gamma(n) q_N^n$$

Then f is meromorphic at each cusp of $\mathbb{H}^*/\Gamma$ means that the Fourier expansion of $f|_k\gamma$ is meromorphic at 0 for each $\gamma \in \mathrm{SL}_2(\mathbb{Z})$, i.e. for each cusp x,

Similarly, we can define modular forms and cusp forms for Γ.

4.2 Modular Curves

For a congruence subgroup Γ, there is a natural quotient map $\mathbb{H}/\Gamma \to \mathbb{H}/\mathrm{SL}_2(\mathbb{Z})$. Every element in the latter space corresponds to an isomorphic class of elliptic curves. It turns out that each point in the former space contains more information.

Given $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_1(N)$ and $\tau \in \mathbb{C}$, let $\Lambda_1 = \Lambda(1, \tau)$ and $\Lambda_2 = \Lambda\big(1, \gamma(\tau)\big)$. Then the isomorphism $\Lambda_1 \to \Lambda_2$ is given by $z \mapsto \frac{z}{c\tau+d}$, inducing a holomorphic isomorphic $\mathbb{C}/\Lambda_1 \to \mathbb{C}/\Lambda_2$ given by $[z] \mapsto [\frac{z}{c\tau+d}]$. We want to determine some point $x + \tau y$ that is invariant under the isomorphism, i.e.

$$\big(x + \gamma(\tau)y\big) - (\frac{x+\tau y}{c\tau+d}) = \frac{\big(cx + (a-1)y\big)\tau + \big((d-1)x + by\big)}{c\tau+d} \in \Lambda_2 = \frac{\Lambda_1}{c\tau+d}$$

Note that $x + y\tau = \frac{1}{N}$ satisfies the equation. Actually for every $T \in E$ of order N, there is $\tau \in \mathbb{H}$ such that $E \cong \mathbb{C}/\Lambda(1,\tau)$ and $T = \frac{1}{N}$ under such isomorphism. Therefore, the map $(\mathbb{C}/\Lambda(1,\tau), \frac{1}{N}) \mapsto [\tau]$ gives a map from isomorphic classes of pairs (E, T) to $\mathbb{H}/\Gamma_1(N)$, where E is an elliptic curve over $\mathbb{C}$ and $T \in E$ is a point of order N. Two pairs $(E, T) \sim (E', T')$ if there is an isomorphism $E \to E'$ sending T to T'. Similarly, we can show that the group $\{0, \frac{1}{N}, \cdots, \frac{N-1}{N}\}$ is fixed by $\Gamma_0(N)$.

Precisely, we have the following theorem:

Theorem 4.3. *Let $N \geqslant 1$ be an integer.*

(a) There is a smooth projective curve $X_1(N)/\mathbb{Q}$ and a complex analytic isomorphism

$$j_{N,1} \colon \mathbb{H}^*/\Gamma_1(N) \to X_1(N)(\mathbb{C})$$

The space $\mathbb{H}/\Gamma_1(N)$ parametrizes isomorphic classes (E, T), where E is an elliptic curve over $\mathbb{C}$ and $T \in E$ is a point of order N. Two pairs $(E, T) \sim (E', T')$ if there is an isomorphism $E \to E'$ sending T to T'.

(b) There is a smooth projective curve $X_0(N)/\mathbb{Q}$ and a complex analytic isomorphism

$$j_{N,0} \colon \mathbb{H}^*/\Gamma_0(N) \to X_0(N)(\mathbb{C})$$

The space $\mathbb{H}/\Gamma_0(N)$ parametrizes isomorphic classes (E, C), where E is an elliptic curve over $\mathbb{C}$ and $C \subset E$ is a cyclic subgroup of order N. Two pairs $(E, C) \sim (E', C')$ if there is an isomorphism $E \to E'$ sending C to C'.

Proof. See [12, Appendix C, Theorem 13.1] for detailed descriptions and further references. □

Remark. *Actually, $\mathbb{H}^*/\Gamma(N)$ is also a smooth projective curve $X(N)/\mathbb{Q}$, but it parametrizes more structures on elliptic curves called Weil pairings. Details can also be found in [12, Appendix C.13].*

*If Γ is an arbitrary congruence subgroup, then there is a projective curve $X(\Gamma)$ defined over some number field and a complex analytic isomorphism $j_\Gamma \colon \mathbb{H}^*/\Gamma \to X(\Gamma)(\mathbb{C})$. Then the curve $X(\Gamma)$ is called a **modular curve**.*

Remark. *For a congruence subgroup Γ, $\mathbb{H}^*/\Gamma$ admits a structure of compact Riemann surface (For example, see [3, Chapter 2]). It is well-known that compact Riemann surfaces are the same with projective smooth curves (For example, see [8, Theorem 7.5]). Thus, the nontrivial part of the above theorem is that $X_0(N), X_1(N)$ are curves over $\mathbb{Q}$, i.e. they are given by homogeneous polynomials over $\mathbb{Q}$.*

Next we want to focus on the case $\Gamma = \Gamma_0(N)$. We aim to give some descriptions of $X_0(N)$. First, we need to convert our objects from curves to their function fields.

Proposition 4.4. *Let K be a field of characteristic 0. There is an equivalence of categories between the category of smooth projective curves defined over K with surjective morphisms defined over K and the category of finitely generated extensions L/K of transcendence degree 1 with $L \cap \bar{K} = K$ with field injections fixing K. The equivalence is given by*

$$\begin{aligned} C/K &\mapsto K(C) \\ \phi \colon C_1 \to C_2 &\mapsto \phi^* \colon K(C_2) \to K(C_1) \end{aligned}$$

Proof. See [5, Section I.6]. □

What is the function field of $X_0(N)$? By definition, it is the field of rational functions on a smooth projective curve $X_0(N)$, which are locally fractions of polynomials. This is similar to meromorphic functions on $\mathbb{H}^*/\Gamma_0(N)$ (modular functions for $\Gamma_0(N)$ of weight 0), which are

locally fractions of holomorphic functions on a Riemann surface (a connected one-dimentional complex manifold). In face, the two are the same:

Theorem 4.5. *Let X be a compact Riemann surface. Then the field of meromorphic functions on X is the same with the function field of X.*

Proof. See [9, Chapter 7, Theorem 4] □

Now we have the following description of the function field $\mathbb{C}\big(X_0(N)\big)$ of $X_0(N)$:

Theorem 4.6. *The field $\mathbb{C}\big(X_0(N)\big) = \mathbb{C}\big(j(z), j(Nz)\big)$. The minimal polynomial of $F(j, Y) \in \mathbb{C}(j)[Y]$ of $j(Nz)$ over $\mathbb{C}(j)$ is a polynomial in j has coefficients in $\mathbb{Z}$, i.e. $F(X, Y) \in \mathbb{Z}[X, Y]$. When $N > 1$, F is symmetric in X, Y. Moreover,*

(a) If N is not a perfect square, then $F(X, X)$ is a polynomial of degree > 1 whose leading coefficients is ± 1.

(b) If N is a prime number p, then $F(X, Y) \equiv (X^p - Y)(X - Y^p) \pmod{p}$.

Proof. For detailed proof, see [8, Theorem 6.1] and [2, Theorem 11.18].

In this sketch proof, 'modular function' just means 'modular function of weight 0'.

First, $j(z)$ is invariant under $\Gamma_0(N)$, so $j \in \mathbb{C}\big(X_0(N)\big)$. Let $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N)$ with $c = Nc'$. Then $\begin{pmatrix} a & Nb \\ c' & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$, so

$$j(N\gamma z) = j\left(\frac{Naz + Nb}{cz + d}\right) = j\left(\frac{Naz + Nb}{Nc'z + d}\right) = j(Nz)$$

Thus, $\mathbb{C}\big(j(z), j(Nz)\big) \subset \mathbb{C}\big(X_0(N)\big)$.

Let $\{\gamma_1, \cdots, \gamma_\mu\} \subset \mathrm{SL}_2(\mathbb{Z})$, such that $\mathrm{SL}_2(\mathbb{Z}) = \cup_{i=1}^{\mu} \Gamma_0(N)\gamma_i$. For any modular function $f(z)$ of weight 0 for $\Gamma_0(N)$, the coefficients of the polynomial $\prod_{i=1}^{\mu}\big(Y - f(N\gamma_i z)\big)$ are symmetric polynomials in $f(\gamma z)$. Since the action of $\mathrm{SL}_2(\mathbb{Z})$ permutes $\{f(N\gamma_i z)\}$, coefficients of $\prod_{i=1}^{\mu}\big(Y - f(N\gamma_i z)\big)$ are modular functions for $\mathrm{SL}_2(\mathbb{Z})$, so is a rational function of j by [11, Chapter VII, Section 3, Proposition 6]. Thus, $[\mathbb{C}\big(X_0(N)\big) : \mathbb{C}(j)] \leqslant \mu$. It can be shown that $F(j, Y) = \prod_{i=1}^{\mu}\big(Y - j(N\gamma_i z)\big)$ is the minimal polynomial of $j(Nz)$ over $\mathbb{C}(j)$. Thus, $\mathbb{C}\big(X_0(N)\big) = \mathbb{C}\big(j(z), j(Nz)\big)$. Note that the coefficients of $F(j, Y)$ are holomorphic on $\mathbb{H}$, so they are polynomials in j, so $F(X, Y) \in \mathbb{C}[X, Y]$. Other arguments follow from detailed investigations of the q-expansion of $j(N\gamma z)$. □

We call F the **modular equation**. Since F is irreducible over $\mathbb{C}(X)[Y]$, F is irreducible over $\mathbb{C}[X,Y]$. Let C be the curve in $\mathbb{Q}^2$ given by F. The curve C may not be smooth, but we have a method called blow-up that can produce another smooth curve without changing the function field (For example, see [4, Chapter 7]). We can embed the curve after blow-up into a projective space and take the completion. The above operations do not change the function field (birationally equivalent), so we get a smooth projective curve $\overline{C}$. Let $\overline{C}_{\mathbb{C}}$ be the curve defined by $\overline{C}$ over $\mathbb{C}$. Then

$$\mathbb{C}(C_{\mathbb{C}}) = \mathrm{Frac}\big(\mathbb{C}[X,Y]/F(X,Y)\big) \cong \mathbb{C}\big(j(z)\big)[Y]/F(j,Y) = \mathbb{C}\big(X_0(N)\big)$$

We call $X_0(N)_{\mathbb{Q}} := \overline{C}$ the **canonical model** of $X_0(N)$. On an open subset, the isomorphism from $\mathbb{H}^*/\Gamma_0(N)$ to $\overline{C}_{\mathbb{C}}$ is $[z] \mapsto \big(j(z), j(Nz)\big)$.

4.3 Modularity Theorem

This section is just a short introduction to a more advanced topic. For further references and vivid and detailed descriptions, see [12, Appendix C.13] or [6, Chapter 16 and Chapter 18].

Recall that in [11, Chapter VII, Section 5.4], for an eigenfunction $f = \sum_{n=0}^{\infty} c(n)q^n$ of all $T(n)$ that is a modular form for $\mathrm{SL}_2(\mathbb{Z})$ of weight $2k$, there is an associated Dirichlet series

$$L(f,s) := \Phi_f(s) = \sum_{n=1}^{\infty} \frac{c(n)}{n^s} = \prod_{p\text{: prime number}} \frac{1}{1 - c(p)p^{-s} + p^{2k-1-2s}}$$

There is a similar definition for modular forms for $\Gamma_0(N)$.

For an elliptic curve E over $\mathbb{Q}$, we can associate an L-function to E as follows:

$$L(E,s) := \prod_{p\text{: prime number}} \frac{1}{1 - a_p p^{-s} + \chi(p)p^{1-2s}}$$

where $\chi(p) = 1$ and $a_p = p + 1 - \#E(\mathbb{F}_p)$ for all but finitely many prime number p, where $E(\mathbb{F}_p)$ is the elliptic curve obtained by reducing E to $\mathbb{F}_p$ (Recall that E is defined over $\mathbb{Q}$ means that the Weierstrass equation has coefficients in $\mathbb{Q}$. We can make a change of variable to make the coefficients in $\mathbb{Z}$. Then projects it to $\mathbb{Z}/p\mathbb{Z}$).

Definition 4.7. For an elliptic curve E, we say E is **modular** if there is a surjective morphism $X_0(N) \to E$.

Theorem 4.8. *If an elliptic curve over $\mathbb{Q}$ is modular, then there is a normalized cusp form f for $\Gamma_0(N)$ of weight 2 such that $L(f,s) = L(E,s)$. (See [6, Chapter 16, Theorem 7.4])*

Theorem 4.9 (Taniyama-Shimura-Weil Conjecture, Modularity Theorem)**.** *Every elliptic curve over $\mathbb{Q}$ is modular.*

The conjecture was originally suggested by Taniyama Yutaka and a more precise version by Shimura Goro. André Weil provided significant evidence for the validity of the conjecture. The proof of the conjecture for semi-stable elliptic curves was originally offered by Andrew Wiles in 1993, but a gap was discovered and Wiles fixed it with Richard Taylor in 1995. Following Wiles's ideas, the full version of the conjecture was proved by Christophe Breuil, Brian Conrad, Fred Diamond, Richard Taylor.

The conjecture has deep relation with Fermat's Last Theorem, that is the motivation of Wiles to prove the conjecture. In 1986, Gerhard Frey conjectured that if $a^p + b^p = c^p$ with $abc \neq 0$ and $p \geqslant 3$ prime, the elliptic curve $y^2 = x(x + a^p)(x - b^p)$ could not be modular. The conjecture was progressed by Jean-Pierre Serre and finally proved by Kenneth Ribet. Therefore, if the Modularity Theorem is true, then there cannot be any nontrivial solution to $a^p + b^p = c^p$, so to $a^n + b^n = c^n$ for any $n \in \mathbb{Z}_{>0}$, this implies the Fermat's Last Theorem.

References

[1] Jose Barrios. A brief history of elliptic integral addition theorems. https://scholar.rose-hulman.edu/cgi/viewcontent.cgi?article=1148&context=rhumj, 2009. 1.2

[2] David A. Cox. *Primes of the form = $x^2 + ny^2$: Fermat, class field theory, and complex multiplication*. Pure and Applied Mathematics. Wiley, Hoboken, New Jersey, second edition. edition, 2013. 4.6

[3] Fred Diamond and Jerry Shurman. *A First Course in Modular Forms*. Springer New York, New York, NY, 2016. 4.2

[4] William Fulton. Algebraic curves. http://www.math.lsa.umich.edu/~wfulton/CurveBook.pdf, 2008. 2.3, 4.2

[5] Robin. Hartshorne. *Algebraic Geometry*. Graduate Texts in Mathematics, 52. Springer New York, New York, NY, 1st ed. 1977. edition, 1977. 4.4

[6] Dale. Husemöller. *Elliptic Curves*. Graduate Texts in Mathematics, 111. Springer New York, New York, NY, 2nd ed. 2004. edition, 2004. 4.3, 4.8

[7] Neal Koblitz. *Introduction to Elliptic Curves and Modular Forms*. Graduate texts in mathematics ; Volume 97. Springer Science+Business Media, LLC, New York, second edition. edition, 1993.

[8] James Milne. Modular functions and modular forms (elliptic modular curves). https://www.jmilne.org/math/CourseNotes/MF.pdf, 2017. (document), 4.2, 4.6

[9] R Narasimhan. *Compact Riemann Surfaces*. Lectures in Mathematics. ETH Zurich. Birkhauser, 2012. 4.5

[10] Adrian Rice and Ezra Brown. Why ellipses are not elliptic curves. *Mathematics magazine*, 85(3):163–176, 2012. 1.1, 2

[11] J-P. Serre. *A Course in Arithmetic*. Graduate Texts in Mathematics, 7. Springer New York, New York, NY, 1st ed. 1973. edition, 1973. 4, 4.6, 4.3

[12] Joseph H. Silverman. *The Arithmetic of Elliptic Curves*. Graduate Texts in Mathematics, 106. Springer New York, 2nd ed. 2009. edition, 2009. (document), 1.2, 1.6, 2.2, 3.1, 4.3, 4.2, 4.3