UNIFORMIZATION OF ELLIPTIC CURVES

by

ÖZGE ÜLKEM

Submitted to the Graduate School of Engineering and Natural Sciences
in partial fulfillment of
the requirements for the degree of
Master of Science

Sabancı University
August 2015

TITLE OF THE THESIS/DISSERTATION

APPROVED BY:

Prof. Dr. Henning Stichtenoth
(Thesis Supervisor)

Assoc. Prof. Dr. Alp Bassa (Thesis Co-advisor) A. Bassa

Prof. Dr. Alev Topuzoğlu

Assoc. Prof. Dr. Cem Güneri

Assoc. Prof. Dr. Özgür Gürbüz

DATE OF APPROVAL: 04/08/2015

Özge Ülkem

Mathematics, Master Thesis, 2015

Thesis Supervisor: Prof. Dr. Henning Stichtenoth

Thesis Co-supervisor: Assoc. Prof. Dr. Alp Bassa

Keywords: Elliptic curve, uniformization, lattice, Tate curve

Abstract

Every elliptic curve E defined over $\mathbb{C}$ is analytically isomorphic to $\mathbb{C}^*/q^{\mathbb{Z}}$ for some $q \in \mathbb{C}^*$. Similarly, Tate has shown that if E is defined over a p-adic field K, then E is analytically isomorphic to $K^*/q^{\mathbb{Z}}$ for some $q \in K^*$. Further the isomorphism $E(\overline{K}) \cong \overline{K}^*/q^{\mathbb{Z}}$ respects the action of the Galois group $G_{\overline{K}/K}$, where $\overline{K}$ is the algebraic closure of K. I will explain the construction of this isomorphism.

ELLİPTİK EĞRİLERİN ÜNİFORMİZASYONU

Özge Ülkem

Matematik, Yüksek Lisans Tezi, 2015

Tez Danışmanı: Prof. Dr. Henning Stichtenoth
Tez Eş-Danışmanı: Asist. Prof. Dr. Alp Bassa

Anahtar Kelimeler: Eliptik eğri, ızgara, üniformizasyon, Tate eğrisi

Özet

Kompleks sayılar üzerinde tanımlanan her eliptik eğrin sıfır olmayan bir q kompleks sayısı için $\mathbb{C}/^{\mathbb{Z}}$ yapısına izomorfiktir. Benzer şekilde, Tate göstermiştir ki p-adic bir K cismi üzerinde tanımlanan br E eliptik eğrisi de $q \in K^*$ olmak üzere, $K^*/q^{\mathbb{Z}}$ yapısına izomorfiktir. Dahası, $E(\overline{K}) \cong \overline{K}^*/q^{\mathbb{Z}}$ izomorfizması $\overline{K}$, K'nin cebirsel kapanı ş ı olmak üzere $G_{\overline{K}/K}$ Galois grubunun etkisine saygı duyar. Bu tezde bu izomorfizmaları kuracağız.

Contents

CHAPTER 1

Introduction

In this thesis, I will consider elliptic curves over $\mathbb{C}$ and over $\mathbb{Q}_p$, which is the completion of the field $\mathbb{Q}$ of rational numbers under a p-adic valuation.

In the Chapter I we will give some basic definitions and propositions that we will need.

In Chapter II, we will consider the set of elliptic curves over $\mathbb{C}$ as a whole. We will take the collection of $\mathbb{C}$-isomorphism class of elliptic curves and make it into an algebraic curve, which is an example of a modular curve. Then by studying functions on this modular curve we will construct a bijection between the isomorphism classes of elliptic curves and the homothety classes of lattices. This is called the uniformization of elliptic curves over $\mathbb{C}$.

In Chapter III, we will consider elliptic curves defined over a p-adic field K, which is a finite extension of $\mathbb{Q}_p$. We will describe Tate's theory of these elliptic curves and we will derive a uniformization of elliptic curves over K.

CHAPTER 2

Preliminaries

2.1 Elliptic Curves

Let K be a field and $\overline{K}$ be the algebraic closure of K. Consider a curve E over K given by the equation

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \tag{1}$$

where $a_1, \ldots, a_6 \in \bar{K}$.

If $char(K) \neq 2$, we can simplify the equation above by completing squares. Replacing y by $\frac{1}{2}(y - a_1x - a_3)$ gives an equation of the form

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

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

Also, define $b_8 = a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2$
$c_4 = b_2^2 - 24b_4$

Definition 2.1 *The discriminant of this curve defined by the equation above is defined by the quantity:*

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

Definition 2.2 *We call the curve given by an equation of the form (1) an elliptic curve if* $\Delta \neq 0$.

Definition 2.3 *The quantity $j = \frac{c_4^3}{\Delta}$ is called the j-invariant of the curve E defined above.*

As it is customary, we will consider the curve E as a projective curve with its points at infinity in the projective plane. It can be checked easily that a curve defined by equation as given above has a unique point at infinity with projective coordinates $[0 : 1 : 0]$. We will denote this point by O and call it base point of E. We will define a group operation on E. Take any $P, Q \in E$. Let L be the line connecting P and Q (tangent line to E if $P = Q$). By BÃl'zout theorem, L intersect the curve E at a third point. Denote this third point by R. Let L' be be the line connecting R and O. Then, $P \oplus Q$ is the point such that L' intersects E at R, O and $P \oplus Q$.

Proposition 2.4 *Let E be an elliptic curve with the base point $O = [0, 1, 0]$. Then, E is an abelian group under the operation $\oplus$, where the identity element of this group is O.*

Proof: [5, Chapter III, Section 2]

Group Law Formula

Let E be an elliptic curve given by
$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$.
(a) Let $P_0 = (x_0, y_0) \in E$. Denote by $\ominus P_0$ the additive inverse of $P_0 = (x_0, y_0)$. It is given by $\ominus P_0 = (x_0, -y_0 - a_1x_0 - a_3)$.
Let $P_1 \oplus P_2 = P_3$ with $P_i = (x_i, y_i) \in E$.
(b) If $x_1 = x_2$ and $y_1 + y_2 + a_1x_2 + a - 3 = 0$ then $P_1 \oplus P_2 = O$.
Otherwise, let
$\lambda = \frac{y_2 - y_1}{x_2 - x_1}, \quad \nu = \frac{y_1x_2 - y_2x_1}{x_2 - x_1}$ if $x_1 \neq x_2$
$\lambda = \frac{3x_1^3 + 2a_2x_1 + a_4 - a_1y_1}{2y_1 + a_1x_1 + a_3}, \quad \nu = \frac{-x_1^3 + a_4x_1 + 2a_6 - a_3y_1}{2y_1 + a_1x_1 + a_3}$ if $x_1 = x_2$
(Then, $y = \lambda x + \nu$ is the line through P_1, P_2, or tangent to E if $P_1 = P_2$)
(c) $P_3 = P_1 \oplus P_2$ is given by $x_3 = \lambda^2 + a_1\lambda - a_2 - x_1 - x_2$
$y_3 = -(\lambda + a_1)x_3 - \nu - a_3$.

Definition 2.5 *For projective curves E, E', a morphism $\phi : E \longrightarrow E'$ is defined by a polynomial mapping*

$$\phi : [X : Y : Z] \mapsto [\phi_0(X, Y, Z) : \phi_1(X, Y, Z) : \phi_2(X, Y, Z)]$$

where ϕ_i are homogeneous polynomials of equal degree such that $[\phi_0(X, Y, Z) : \phi_1(X, Y, Z) : \phi_2(X, Y, Z)]$ satisfies the equation which defines E' for any $[X : Y : Z] \in E$.

To every morphism of curves we can associate an integer called its *degree*.

Definition 2.6 *The degree of $\phi : E \longrightarrow E'$ is the degree of the function field extension $K(E')/K(E)$ induced by ϕ.*

A **homomorphism of elliptic curves** is a morphism of elliptic curves that respects the group structure of the curves.

An **isomorphism of elliptic curves** is a morphism of degree 1.

Later on, we will see that there is a relation between "lattices" over $\mathbb{C}$ and elliptic curves defined over $\mathbb{C}$. This relation is given by "Weierstaß $\wp-$function".

Definition 2.7 *A discrete subgroup of $\mathbb{C}$ which contains an $\mathbb{R}$-basis for $\mathbb{C}$ is called a lattice. And, the number of basis is called the rank of the lattice.*

Definition 2.8 *Let Λ_1, Λ_2 be two lattices. We say Λ_1 and Λ_2 are homothetic if there is a $c \in \mathbb{C}^*$ with $c\Lambda_1 = \Lambda_2$.*

Definition 2.9 *An elliptic function (relative to the lattice Λ) is a meromorphic function $f(z)$ on $\mathbb{C}$ which satisfies*

$$f(z+w) = f(z)$$

for all $w \in \Lambda, z \in \mathbb{C}$.

Definition 2.10 *Let $\Lambda \subset \mathbb{C}$ be a lattice.*

(i) The function

$$\wp(z;\Lambda) = \frac{1}{z^2} + \sum_{w\in\Lambda\setminus\{0\}} \left(\frac{1}{(z-w)^2} - \frac{1}{w^2}\right)$$

is called the Weierstraß $\wp$-function associated to the lattice Λ.

(ii) The Eisenstein series of weight 2k, k>1 (for Λ) is the series

$$G_{2k}(\Lambda) = \sum_{w\in\Lambda\setminus\{0\}} w^{-2k}.$$

Theorem 2.11 *Let $\Lambda \subset \mathbb{C}$ be a lattice.*

(i) The Eisenstein series $G_{2k}(\Lambda)$ for Λ is absolutely convergent for all $k > 1$.

(ii) The series defining the Weierstraß $\wp$-function converges absolutely and uniformly on every compact subset of $\mathbb{C} - \Lambda$. It defines a meromorphic function on $\mathbb{C}$ having a double pole with residue 0 at each lattice point, and no other poles.

(iii) The Weierstraß $\wp$-function is an even elliptic function.

Proof: [5, Chapter VI, Section 3]

2.2 Foundations of Valuation Theory

Definition 2.12 *Let A be a ring. A valuation v is a map*

$$v : A \longrightarrow \mathbb{R}\bigcup\{\infty\}$$

such that

(i) $v(xy) = v(x) + v(y)$

(ii) $v(x+y) \geq min\{v(x), v(y)\}$

with $v(x) = \infty \Leftrightarrow x = 0$. Here ∞ is an abstract element added to $\mathbb{R}$ satisfying $\infty + \infty = \alpha + \infty = \infty + \alpha = \infty$ for $\alpha \in \mathbb{R}$

The following are immediate consequences of the definition:

1. $v(1) = 0$.

2. $v(x^{-1}) = -v(x)$ for $x \in A$.

3. $v(-x) = v(x)$ for $x \in A$.

4. Take any $x, y \in A$. If $v(x) \neq v(y)$, $v(x+y) = min\{v(x), v(y)\}$.

Let K be the field of fractions of the ring A, i.e,

$$K = \{\frac{a}{b} | a, b \in A, b \neq 0\}.$$

Proposition 2.13 *There exists a unique valuation on K which extend v. This valuation is defined as follows:*

$$v(\frac{x}{y}) = v(x) - v(y).$$

Proof: Follows directly from the definition of field of fractions and the identity $a = \frac{a}{b} \cdot b$

By this proposition, without loss of generality, we will focus on valuations on the field K.

Definition 2.14

(i) Let K be a ring with valuation v. The valuation v is called discrete if $v(K^*) = s\mathbb{Z}$ for a real $s > 1$.

(ii) A discrete valuation v is called normalized if $s = 1$.

Definition 2.15 *Let v be a discrete valuation on the field K.*
(i) $\mathcal{O} := \{x \in K | v(x) \geq 0\}$.
The set $\mathcal{O}$ is called the ring of integers of K with respect to the valuation v.
(ii) $\mathcal{P} := \{x \in K | v(x) > 0\}$.
The set $\mathcal{P}$ is called the ideal of the valuation v.
(iii) The set $\mathcal{O}^* = \mathcal{O} \backslash \mathcal{P} = \{x \in K | v(x) = 0\}$ is the set of invertible elements of the ring $\mathcal{O}$
(iv) The field $k = \mathcal{O}/\mathcal{P}$ is called the residue field of the valuation v.

Proposition 2.16 *(i) $\mathcal{P}$ is a principal ideal of $\mathcal{O}$.*
(ii) $\mathcal{O}$ is a local ring and $\mathcal{P}$ is its unique maximal ideal.

Proof:

(i) Before we give the proof, we need

Lemma: Let v be a normalized valuation on K. Then, any nonzero element $x \in K$ can be written as $x = ut^n$, where $t \in \mathcal{P}$ with $v(t) = 1$, $u \in \mathcal{O}^*$ and $n \in \mathbb{Z}$.

Proof of Lemma: Since $v(K^*) = \mathbb{Z}$, there exists an element $t \in K$ with $v(t) = 1$. So, $t \in \mathcal{P}$. Take any $0 \neq x \in K$. Then, $v(x) = m$ for some $m \in \mathbb{Z}$. Hence, $v(xt^{-m}) = 0$ and so $u := xt^{-m} \in \mathcal{O}^*$.

Finally, $x = ut^m$.

Now, take any $0 \neq x \in \mathcal{P}$ such that $n := v(x) \leq v(y)$ for all $y \in \mathcal{P}$. By the lemma above, $x = ut^n$ for the element $t \in \mathcal{P}$ and for some $u \in \mathcal{O}^*$. Hence, $t^n\mathcal{O} \subset \mathcal{P}$.

Conversely, take any $y \in \mathcal{P}$. Again by the lemma, we can write $y = wt^m$, where $t \in \mathcal{P}$ and for some $w \in \mathcal{O}^*$. Since $y \in \mathcal{P}$, we have $m := v(y) \geq v(x) = m$, so we can write

$$y = (wt^{m-n})t^n \in t^n\mathcal{O},$$

hence $\mathcal{P} \subset t^n\mathcal{O}$.

(ii) One can easily show that $\mathcal{P}$ is an ideal of $\mathcal{O}$.

Claim 1 *$\mathcal{P}$ is a maximal ideal of $\mathcal{O}$.*

Proof of Claim 1: Assume A is an ideal of $\mathcal{O}$ with $\mathcal{P} \subsetneq A$. So, there exists $x \in \mathcal{O}^* \cap A$. Then, $1 \in A$ and hence $A = \mathcal{O}$. Therefore, $\mathcal{P}$ is a maximal ideal of $\mathcal{O}$.

Claim 2 *$\mathcal{P}$ is the unique maximal ideal.*

Proof of Claim 2: Assume now there exists a maximal ideal B of $\mathcal{O}$ such that $B \neq \mathcal{P}$. Then, $B \cap \mathcal{O}^* = \{0\}$. Hence, for any nonzero element $x \in B$, we have $v(x) > 0$, which implies that $B \subset \mathcal{P}$, contradiction.

By the previous proposition, we know that $\mathcal{P}$ is generated by one element, say t, i.e, $\mathcal{P} =< t >$. The element t is called a uniformizing parameter for the valuation v.

Example 2.17 *Let $\mathbb{Q}$ be the field of rational numbers. Take any $q \in \mathbb{Q}\backslash\{0\}$. Then, we can express q as a product of powers of prime numbers: $q = \pm p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_n^{\alpha_n}$ for some prime numbers $p_1, \ldots, p_n$ where $\alpha_1, \ldots, \alpha_n \in \mathbb{Z}$. If v is a valuation on $\mathbb{Q}$, then it is sufficient to know v on prime numbers since $v(q) = \alpha_1 v(p_1) + \cdots + \alpha_n v(p_n)$.*

If there is no prime number p with $v(p) > 0$, then $v(q) = 0$. Now assume there exists a prime number with positive valuation.

***Claim**: There exists at most one prime number p with $v(p) > 0$.*

Prrof of the Claim: Assume there exists two primes p_1, p_2 suvh that $v(p_1) > 0$ and $v(p_2) > 0$. Since $gcd(p_1, p_2) = 1$, there are $a, b \in \mathbb{Z}$ such that $ap_1 + bp_2 = 1$.

$\Longrightarrow 0 = v(1) = v(ap_1 + bp_2) \geq min\{v(ap_1), v(bp_2)\} > 0$

Let p be a prime number. Define, $v(p) := 1$ and for $m \in \mathbb{Q}$, define $v(m) := \alpha$ where α is the biggest power of p dividing m. Then, v gives us a valuation on $\mathbb{Q}$

And, p is a uniformizing element and the residue field of $\mathbb{Q}$ with this valuation is $\mathbb{Z}/ < p >$.

Definition 2.18 *An absolute value of K is a function*

$$|.| : K \to \mathbb{R}$$

satisfying for all $x, y \in K$

(i) $|x| = 0 \iff x = 0$

(ii) $|x| \geq 0$

(iii) $|xy| = |x|.|y|$

(iv) $|x+y| \leq |x| + |y|$

Definition 2.19 *An absolute value is called non-Archimedean if it satisfies $|x + y| \leq max\{|x|, |y|\}$ for all $x, y \in K$.*

An absolute value gives a topological structure on K by the metric $d(x, y) = |x - y|$. So, we can talk about notions as convergence of series and dense subsets.

2.2.1 Relation between non-Archimedean absolute value and Valuation

Theorem 2.20 *Let $|.|$ be an absolute value on K and $s \in \mathbb{R}, s > 0$. Then the function*

$$v_s : K \longrightarrow \mathbb{R} \cup \{\infty\}$$
$$x \mapsto \begin{cases} -slog|x| & if \quad x \neq 0 \\ \infty & if \quad x = 0 \end{cases}$$

is a non-archimedean valuation on K.

Conversely, if v is a valuation on K and $q \in \mathbb{R}, q > 1$ the function

$$|.|_q : K \longrightarrow \mathbb{R}$$
$$x \mapsto \begin{cases} q^{-v(x)} & if \quad x \neq 0 \\ 0 & if \quad x = 0 \end{cases}$$

is an absolute value on K.

Definition 2.21 *Let K be a field with an absolute value $|\cdot|$. A sequence (a_n) called a Cauchy sequence if for all $\epsilon > 0$, there exists $N \in \mathbb{N}$ such that for all $n, m > N$,*

$$|a_n - a_m| < \epsilon.$$

Definition 2.22 *A field K with an absolute value $|.|$ is called complete if any Cauchy sequence (a_n) converges to an element $a \in K$.*

Theorem 2.23 *Let K be a field with an absolute value $|.|$ on K. Then, there exists a complete field $\widehat{K}$ with an absolute value $|.|_{\widehat{K}}$ such that K is embedded in $\widehat{K}$ as a dense subfield and $|x|_{\widehat{K}} = |x|$ if $x \in K$. The field $\widehat{K}$ is unique up to continuous K-isomorphism and hence is called the completion of K.*

Proof : [2, Chapter II, Section 4]

Theorem 2.24 *Let K be a valued field and $\widehat{K}$ be its completion with respect to the valuation v on K. Denote by $\widehat{v}$ the corresponding valuation on $\widehat{K}$. Let*

$\mathcal{O}$ (respectively $\widehat{\mathcal{O}}$) be the valuation ring of K (respectively, $\widehat{K}$)

$\mathcal{P}$ (respectively $\widehat{\mathcal{P}}$) be the maximal ideal of $\mathcal{O}$ (respectively $\widehat{\mathcal{O}}$)
and
$\mathcal{K}$ (respectively, $\widehat{\mathcal{K}}$) be the residue field.
Then,
$\mathcal{K} \cong \widehat{\mathcal{K}}$
if v is discrete then $\mathcal{O}/\mathcal{P}^n \cong \widehat{\mathcal{O}}/\widehat{\mathcal{P}}^n$, where $n \geq 1$.

Proof: [2, Chapter I, Section 3]

Theorem 2.25 *Take the same assumptions as in the previous theorem. Assume also v is normalized. Let $R \subset \mathcal{O}$ be a set of representatives of $\mathcal{K}$ such that $0 \in R$ and let $t \in \mathcal{P}$ be a uniformizing element. Then, we can represent all $x \in \widehat{K}^*$ as a convergent series*

$$x = t^m(a_0 + a_1 t + a_2 t^2 + \dots)$$

with $a_i \in R, i \in \mathbb{N}, a_0 \neq 0$ and $m \in \mathbb{Z}$.

Proof: Take any $x \in \widehat{K}^*$. Since t is a uniformizing element, we have $x = ut^m$ where $u \in \widehat{\mathcal{O}}^*$. Since $\mathcal{O}/\mathcal{P} \cong \widehat{\mathcal{O}}/\widehat{\mathcal{P}}$ by the previous theorem, $u \bmod \widehat{\mathcal{P}}$ has a representative $0 \neq a_0 \in R$ and hence we can write $u = a_0 + tb_1$ with $b_1 \in \widehat{\mathcal{O}}$.

By induction, there exists $a_1, \dots, a_n \in R$ such that

$$u = a_0 + a_1 t + \dots + a_{n-1}t^{n-1} + t^n b_n$$

with $b_n \in \widehat{\mathcal{O}}$.

Similarly, there exists $a_n \in R$ such that $b_n = a_n + tb_{n+1}$ where $b_{n+1} \in \widehat{\mathcal{O}}$.

Hence,

$$u = a_0 + a_1 t + \dots + a_{n-1}t^{n-1} + a_n t^n + t^{n+1} b_{n+1}.$$

We can do this for all $n \in \mathbb{N}$. Hence, we obtain a series $\sum_{n=0}^{\infty} a_n t^n$.

Claim: This series converges to u.

Proof of the Claim: For any $n \in \mathbb{N}$, we have

$$\widehat{v}(u - \sum_{i=1}^{n} a_n t^n) = \widehat{v}(t^{n+1}b_{n+1}) = \widehat{v}(t^{n+1}) + \widehat{v}(b_{n+1}) = n + 1 + \widehat{v}(b_{n+1}) \geq n + 1.$$

Therefore, we get

$$\lim_{n\to\infty} \widehat{v}(u - \sum_{i=0}^{n} a_i t^i) = \infty.$$

Hence, the series converges to u and so we are done.

Example 2.26 *Consider the valuation on $\mathbb{Q}$ defined in the Example 1.17.*

Denote by $\mathbb{Q}_p$ the completion of $\mathbb{Q}$ with respect to the valuation v_p.

We will use also v_p for the extension of v_p to $\mathbb{Q}_p$.

Denote by $\mathcal{K}_p$ the residual field $\mathcal{O}/\mathcal{P}$ where $\mathcal{O}$ is the valuation ring and $\mathcal{P}$ is its unique maximal ideal. Clearly, $\mathcal{P}$ is generated by the prime number p.

***Claim**: $\mathcal{K}_p \cong \mathbb{Z}/p\mathbb{Z}$.*

Proof of the Claim: Follows from Theorem 1.24.

By the claim, we can take $\{0,\dots,p-1\}$ as set of representatives of $\mathcal{K}_p$. According to the theorem, for any $0 \neq x \in \mathbb{Q}_p$, we have

$$x = p^m(a_0 + a_1 p + a_2 p^2 + \dots) = \sum_{i=0}^{\infty} a_i p^{i+m}$$

with $a_i \in \{0,\dots,p-1\}, i \in \mathbb{N}, a_0 \neq 0$ and $m \in \mathbb{Z}$.

Also, by the construction of the same theorem, we know

$$u = a_0 + a_1 p + \dots = \sum_{i=0}^{\infty} a_i p^i$$

is a unit, i.e., $v_p(u) = 0$. Hence, $v_p(x) = m$.

Therefore, the valuation ring of $\mathbb{Q}_p$ is

$$\mathbb{Z}_p = \{\sum_{i=m}^{\infty} a_i p^i | a_i \in \{0,\dots,p-1\}, m \geq 0\},$$

with the unique maximal ideal $p\mathbb{Z}_p$.

$\mathbb{Z}_p$ is called the ring of p-adic integers

Example 2.27 *Let K be a field and $K((x))$ be the field of formal power series over K.*

Take any $f(x) \in K((x))$, $f(x) = \sum_{r=m}^{\infty} a_r x^r$. Define a function $v : K((x)) \longrightarrow \mathbb{R} \cup \{\infty\}$ as follows:

$v(f(x)) = t$, where a_t is the first nonzero coefficient in f, if f is a nonzero element in $K((x))$ and $v(0) = \infty$. It can be easily seen that v is a discrete valuation on $K((x))$.

The valuation ring of $K((x))$ consists of formal power series with nonnegative exponent, with the unique maximal ideal

$$\mathcal{P} = \{f(x) \in K((x)) | \sum_{r=1}^{\infty} a_r x^r\}.$$

So, x is a uniformizing element.

Now we will define a tool for understanding the behaviour of polynomials over a valued field, which is called *Newton Polygon*.

Definition 2.28 *Let K be a valued field with the valuation v defined on it. Take any $f(x) = a_n x^n + \dots + a_1 x + a_0 \in K[x]$ of degree n. The Newton polygon of $f(x)$ is the convex hull of the set of points*

$$\{(j, v(a_j)) | j \geq 0\} \cup \{Y_{+\infty}\}$$

where $Y_{+\infty}$ denotes the set of at infinity of the positive vertical axis (i.e, if $a_j = 0$ then $(j, v(a_j)) = Y_{+\infty}$).

We can define the Newton polygon of a power series or Laurent series in a similar way.

Definition 2.29 *Let K be a complete field with respect to valuation v. Let $f(X) = \sum\limits_{n\geq 0} a_n X^n$ with $a_n \in K$. The Newton polygon of f is defined to be the convex hull of the set*

$$\{(j, v(a_j))\}_{j\geq 0} \cup \{Y_{+\infty}\}$$

where $Y_{+\infty}$ defined as before.

Theorem 2.30 *Let K be a complete field and let $f = \sum\limits_{n=0}^{\infty} a_n X^n \in K[[X]]$. Then, to each side of the Newton polygon of f there correspond l zeros (counting multiplicities) of f where l is the lenght of the horizontal projection of the side.*

Proof: [3, Chapter II, Section 2]

Theorem 2.31 (Schnirelmann) *Let $f(X) = \sum\limits_{-\infty}^{+\infty} c_i X^i$ be a formal Laurent series with coefficient c_i in a finite extension K of $\mathbb{Q}_p$. We suppose that $f(X)$ converges for all $\overline{K}^*$. Then, $f(X)$ can be written in the form*

$$f(X) = cX^k \prod_{|\alpha|<1} (1 - \frac{\alpha}{X}) \prod_{|\alpha|<1} (1 - \frac{X}{\alpha})$$

with finite non-empty sets of roots $\alpha \in \overline{K}$ occuring on the critical spheres of f. Gathering these roots of given modulus together, we get a representation

$$f(X) = cX^k \prod_{i<0} \hat{g}_i(X) \prod_{i\geq 0} g_i(X)$$

with polynomials $g_i(X) \in K[X]$ or $\hat{g}_i(X) \in K[X^{-1}]$ having the same roots as f on the critical spheres of radii $r_i, c \in K, k \in \mathbb{Z}$.

Proof: [4, Chapter II,Section 4]

CHAPTER 3

Uniformization of Elliptic Curves over $\mathbb{C}$

It is known that each lattice Λ of rank 2 gives an elliptic curve E defined over $\mathbb{C}$ via the complex analytic map given by the Weierstaß $\wp$-function and its derivative.

Let $\mathcal{L}$ be the set of lattices of rank 2 in $\mathbb{C}$. Then, $\mathbb{C}^*$ acts on $\mathcal{L}$ by multiplication where

$$c\Lambda = \{cw | w \in \Lambda\}$$

for any $c \in \mathbb{C}^*$. This action is called homothety. Since homothetic lattices give isomorphic elliptic curves over $\mathbb{C}$, we have an injection:

$$\mathcal{L}/\mathbb{C}^* \hookrightarrow \{\text{Elliptic curves over } \mathbb{C}\}/\mathbb{C} - isomorphism.$$

Actually, this map is a bijection. Our main aim in this section to prove that it is indeed a bijection.

This is called *Uniformization Theorem of Elliptic Curves over* $\mathbb{C}$.

Let Λ be a lattice in $\mathbb{C}$. Choose a basis for Λ, say ω_1, ω_2. Then,

$$\Lambda = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2,$$

which is homothetic to $\mathbb{Z}\frac{\omega_1}{\omega_2} + \mathbb{Z}$. We choose ω_1 and ω_2 such that the angle between ω_2 and ω_1 is between 0 and π. Since it is enough to consider the lattices up to homothety, let us normalize our lattice

$$\mathbb{Z}\frac{\omega_1}{\omega_2} + \mathbb{Z}.$$

This lattice is homothetic to the lattice

$$\frac{1}{\omega_2}\mathbb{Z} + \mathbb{Z}.$$

Because of the choice of the angle between ω_2 and ω_1, we have $im(\frac{\omega_1}{\omega_2}) > 0$, i.e., $\frac{\omega_1}{\omega_2} \in \mathbf{H}$, where

$$\mathbf{H} = \{z \in \mathbb{C} : im(z) > 0\}.$$

Denote $\frac{w_1}{w_2}$ by τ. So, we can rewrite the lattice $\mathbb{Z}\frac{w_1}{w_2} + \mathbb{Z}$ as $\mathbb{Z}\tau + \mathbb{Z}$. We will denote the latter lattice by Λ_τ. Therefore, there is a natural map:

$$\mathbf{H} \longrightarrow \mathcal{L}/\mathbb{C}^*$$
$$\tau \mapsto \Lambda_\tau$$

This map is surjective.

So, each element τ in the upper half plane gives us a lattice Λ_τ. However, this is not a bijection. When do two elements in the upper plane give the homothetic lattice? The answer will follow from

Lemma 3.1 *Let* $a, b, c, d \in \mathbb{R}$ *with* $ad - bc \neq 0$*,* $\tau \in \mathbb{C}\backslash\mathbb{R}$*. Then,*

$$im(\frac{a\tau + b}{c\tau + d}) = \frac{(ad - bc)im\tau}{|c\tau + d|^2}.$$

Proof: [6, Chapter I, Section 1]

The complication here is choosing a basis for the lattice Λ_τ corresponding to $\tau \in \mathbb{C}$. Let ω_1, ω_2 and ω_1', ω_2' be two bases for the lattice Λ_τ. Then, there are $a, b, c, d, a', b', c', d' \in \mathbb{Z}$ such that

$$\omega_1' = a\omega_1 + b\omega_2 \qquad \omega_1 = a'\omega_1' + b'\omega_2'$$
$$\omega_2' = c\omega_1 + d\omega_2 \qquad \omega_2 = c'\omega_1' + d'\omega_2'.$$

Now, by substituing ω_1 and ω_2 in the expression of ω_1' and ω_2', we get:

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} \omega_1' \\ \omega_2' \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} \begin{pmatrix} \omega_1' \\ \omega_2' \end{pmatrix}$$

And hence,

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}. \tag{3.1}$$

Now, as $im(\frac{\omega_1'}{\omega_2'}) > 0$, by defining $\tau := \frac{\omega_1}{\omega_2}$ and using the previous lemma we get:

$0 < im(\frac{\omega_1'}{\omega_2'}) = im(\frac{a\tau+b}{c\tau+d}) = \frac{(ad-bc)im\tau}{|c\tau+d|^2}$. Hence, $ad - bc > 0$. Moreover, from (1) we have,

$$(ad - bc)(a'd' - b'c') = 1.$$

Since, $a, b, c, d, a', b', c', d' \in \mathbb{Z}$, either $ad - bc = 1 \wedge a'd' - b'c' = 1$ or $ad - bc = -1$ $\wedge\ a'd' - b'c' = -1$. As $ad - bc > 0$, we have $ad - bc = 1$; which means $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$.

Lemma 3.2 *(a) Let* Λ *be a lattice in* $\mathbb{C}$*, say* $\Lambda = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2 = \mathbb{Z}\omega_1' + \mathbb{Z}\omega_2'$*. Then,* $\omega_1' = a\omega_1 + b\omega_2$ *and* $\omega_2' = c\omega_1 + d\omega_2$ *for some* $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$*.*

(b) Take any $\tau_1, \tau_2 \in \mathbf{H}$*. Then,* Λ_{τ_1} *is homothetic to* Λ_{τ_2} *if and only if there exists* $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$ *such that* $\tau_2 = \frac{a\tau_1+b}{c\tau_1+d}$*.*

(c) Let Λ *be a lattice in* $\mathbb{C}$*. Then, there exists an element* $\tau \in \mathbb{C}$ *such that* Λ *is homothetic to* $\Lambda_\tau = \mathbb{Z}\tau + \mathbb{Z}$*.*

Proof: (a) is proved above.

For the proof of (b) and (c), please see [6, Chapter I, Section 1].

By Lemma 2.1, we can define an action of $SL_2(\mathbb{Z})$ on the set $\mathbf{H}$ as follows:

$$SL_2(\mathbb{Z}) \times \mathbf{H} \longrightarrow \mathbf{H}$$

$$\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix}, \tau\right) \mapsto \frac{a\tau + b}{c\tau + d}$$

By this action we have an equivalence relation on $\mathbf{H}$:

We say τ_1 and τ_2 are equivalent if there exists a $\gamma \in SL_2(\mathbb{Z})$ such that $\tau_1 = \gamma\tau_2$ and by Lemma 2.2(b) equivalence classes of $\mathbf{H}$ corresponds to the set of homothetic lattices. Therefore, we have a one-to-one correspondence

$$\mathbf{H}/SL_2(\mathbb{Z}) \longleftrightarrow \mathcal{L}/\mathbb{C}^*$$

We will denote the elements $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ and $\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$ by simply 1 and -1 respectively. Obviously, these elements act on $\mathbf{H}$ trivially. Moreover, these are the only elements in $SL_2(\mathbb{Z})$ which fix $\mathbf{H}$.

Definition 3.3 *The modular group,* $\Gamma(1)$*, is the quotient group* $SL_2(\mathbb{Z})/\{-1, +1\}$*.*

Consider two special elements in $SL_2(\mathbb{Z})$: $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ and $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$. Name them S and T, respectively.

Take any $\tau \in \mathbf{H}$. Then, $S(\tau) = \frac{-1}{\tau}$ and $T(\tau) = \tau + 1$.

Later we will prove that the modular group $\Gamma(1)$ is generated by S and T.

In this section we will be working with the modular group $\Gamma(1)$ and the action of it on the upper half plane $\mathbf{H}$. First, we will give a description of the modular space $\mathbf{H}/\Gamma(1)$.

Proposition 3.4 *Let* $\mathcal{F} \subset \mathbf{H}$ *be the set*

$$\mathcal{F} = \{\tau \in \mathbf{H} : |\tau| \geq 1 \wedge |Re(\tau)| \leq \frac{1}{2}\}.$$

Then;

(a) For any $\tau \in \mathbf{H}$ *there exists* $\gamma \in \Gamma(1)$ *such that* $\gamma.\tau \in \mathcal{F}$*.*

(b) Suppose that both τ *and* $\gamma.\tau$ *are in* $\mathcal{F}$ *for some* $\gamma \in \Gamma(1)$*,* $\gamma \neq 1$*. Then one of the following holds:*

- $Re(\tau) = -\frac{1}{2}$ *and* $\gamma.\tau = \tau + 1$*;*
- $Re(\tau) = \frac{1}{2}$ *and* $\gamma.\tau = \tau - 1$*;*
- $|\tau| = 1$ *and* $\gamma.\tau = \frac{-1}{\tau}$*.*

(c) Take any $\tau \in \mathcal{F}$*. Let* $I(\tau) = \{\gamma \in \Gamma(1) : \gamma.\tau = \tau\}$ *be the stabilizer of* τ*. Then,*

$$I(\tau)=\begin{cases}\{1,S\} & \textit{if} \quad \tau=i\\ \{1,ST,(ST)^2\} & \textit{if} \quad \tau=\rho=e^{\frac{2i\pi}{3}}\\ \{1,TS,(TS)^2\} & \textit{if} \quad \tau=-\bar{\rho}=e^{\frac{2i\pi}{6}}\\ \{1\} & \textit{otherwise}\end{cases}$$

Proof: [6, Chapter I]

Definition 3.5 *The extended upper half plane* $\mathbf{H}^*$ *is the union of the upper half plane* $\mathbf{H}$ *and the* $\mathbb{Q}$*-rational points of the projective line.*

$$\mathbf{H}^*=\mathbf{H}\bigcup\mathbb{Q}\bigcup\{\infty\}$$

We have seen that $SL_2(\mathbb{Z})$ acts on the upper half plane $\mathbf{H}$. We can extend this action to $\mathbf{H}^*$ as follows:

Take any $(x:y)\in\mathbb{P}^1(\mathbb{Q})$ in homogeneous coordinates and let $\gamma=\begin{pmatrix}a & b\\ c & d\end{pmatrix}$. Then.

$$\gamma.(x:y)=(ax+by:cx+by)$$

Now, define $X(1):=\mathbf{H}^*/\Gamma(1)$ and $Y(1):=\mathbf{H}/\Gamma(1)$. The points in $X(1)\backslash Y(1)$ are called the cusps of $X(1)$.

Lemma 3.6 *(a)* $X(1)\backslash Y(1)=\{\infty\}$.

(b) The stabilizer of $\infty\in\mathbf{H}^*$ *in* $\Gamma(1)$ *is*

$$I(\infty)=\left\{\begin{pmatrix}1 & b\\ 0 & 1\end{pmatrix}\in\Gamma(1)\right\}=<T>\leq\Gamma(1)$$

.

We will investigate the structure of $X(1)$.

Definition 3.7 *Let* X *be a topological space. A complex structure on* X *is an open covering* $\{\mathcal{U}_i\}_{i\in I}$ *of* X *and homeomorphisms*

$$\psi_i:\mathcal{U}_i\longrightarrow\psi_i(\mathcal{U}_i)\subset\mathbb{C}$$

such that each $\psi_i(\mathcal{U}_i)$ *is an open subset of* $\mathbb{C}$ *and such that* $\forall i,j\in I$ *with* $\mathcal{U}_i\cap\mathcal{U}_j\neq 0$*, the map*

$$\psi_j\circ\psi_i^{-1}:\psi_i(\mathcal{U}_i\cap\mathcal{U}_j)\longrightarrow\psi_j(\mathcal{U}_i\cap\mathcal{U}_j)$$

is holomorphic.

The map ψ_i *is called a local parameter for the points in* $\mathcal{U}_i$*.*

Definition 3.8 *A Riemann surface is a connected Hausdorff space which has a complex structure defined on it.*

Theorem 3.9 *The following defines a complex structure on* $X(1)$ *which gives it the structure of a compact Riemann surface:*

For $x\in X(1)$*, choose* $\tau_x\in\mathbf{H}^*$ *with* $\phi(\tau_x)=x$ *and let* $\mathcal{U}_x\subset\mathbf{H}^*$ *be a neighborhood of* τ_x *satisfying*

$$I(\mathcal{U}_x, \mathcal{U}_x) = I(\tau_x).$$

Then, $I(\tau_x)\backslash\mathcal{U}_x \subset X(1)$ is a neighborhood of x, so $\{I(\tau_x)\backslash\mathcal{U}_x\}_{x\in X(1)}$ is an open cover of $X(1)$.

$\underline{x \neq \infty}$ *: Let r be the cardinality of $I(\tau_x)$ and let g_x be the holomorphic isomorphism*

$$g_x : \mathbf{H} \longrightarrow \{z \in \mathbb{C} \| z| < 1\}$$

defined by $g_x(\tau) = \frac{\tau - \tau_x}{\tau - \bar{\tau_x}}$

Then, the map $\psi_x : I(\tau_x)\backslash\mathcal{U}_x \longrightarrow \mathbb{C}$ defined by $\psi_x(\phi(\tau)) = g_x(\tau)^r$ is well defined and gives a local parameter at x.

$\underline{x = \infty}$ *: We may take $\tau_x = \infty$, so $I(\tau_x) = \{T^k\}$.*

Then, $\psi_x : I(\tau_x)\backslash\mathcal{U}_x \longrightarrow \mathbb{C}$, $\psi_x(\phi(\tau)) = \begin{cases} e^{2i\pi\tau} & \text{if} \quad \phi(\tau) \neq \infty \\ 0 & \text{if} \quad \phi(\tau) = \infty \end{cases}$

is well defined and gives a local parameter at x.

Proof: [6, Chapter I, Section 2]

After defining complex structure on $X(1)$, we can talk about holomorphic and meromorphic functions.

Definition 3.10 *Let $k \in \mathbb{Z}$ and $f(\tau)$ be a function on* H. *We say that f is weakly modular of weight $2k$ (for $\Gamma(1)$) if*

(i) f is meromorphic on H*,*

(ii) $f(\gamma\tau) = (c\tau + d)^{2k} f(\tau)$ for all $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$.

From (i), we can express f as a function of $q = e^{2i\pi\tau}$ and f will be meromorphic in the punctured disc $\{q : 0 < |q| < 1\}$. Then, f has a Laurent series expression $\widetilde{f}$ in the variable q as

$$\widetilde{f}(q) = \sum_{-\infty}^{\infty} a_n q^n.$$

Definition 3.11 *With the notation above f is said to be*

$\underline{\text{meromorphic at } \infty}$ if $\widetilde{f} = \sum_{-n_0}^{\infty} a_n q^n$ for some $n_0 \in \mathbb{N}$.

$\underline{\text{holomorphic at } \infty}$ if $\widetilde{f} = \sum_{n=0}^{\infty} a_n q^n$.

If f is meromorphic at ∞, say $\widetilde{f} = a_{-n_0} q^{-n_0} + \ldots$ with $a_{-n_0} \neq 0$ then

$$ord_\infty(f) = ord_{q=0}(\widetilde{f}) = -n_0.$$

If f is holomorphic at ∞, its value at ∞ is defined to be $f(\infty) = \widetilde{f}(0) = a_0$.

Definition 3.12 *(i) A weakly modular function that is meromorphic at ∞ is called modular function.*

(ii) A modular function that is everywhere holomorphic is called a modular form.

Definition 3.13 *The modular j-invariant $j(\tau)$ is the function*

$$j(\tau) = 1728\frac{g_2(\tau)^3}{\Delta(\tau)},$$

with $g_2(\tau) = 60G_4(\tau)$ where $G_4(\tau)$ is the Eisenstein series of weight 4.

Therefore, $j(\tau)$ is the j-invariant of the elliptic curve

$$E_{\Lambda_\tau} : y^2 = 4x^3 - g_2(\tau)x - g_3(\tau)$$

and $E_{\Lambda_\tau}(\mathbb{C})$ has a parametrization using the Weierstraß $\wp$-function:

$$\mathbb{C}/\Lambda_\tau \longrightarrow E_{\Lambda_\tau}(\mathbb{C})$$

$$z \mapsto (\wp(z;\Lambda_\tau), \wp'(z;\Lambda_\tau))$$

Theorem 3.14 *$j(\tau)$ is a modular function of weight 0. It induces a (complex analytic) isomorphism $j : X(1) \to \mathbb{P}^1(\mathbb{C})$.*

Proof: [6, Chapter I, Section 4]

Theorem 3.15 (Uniformization Theorem for Elliptic Curves over $\mathbb{C}$) *Let A,B $\in \mathbb{C}$ satisfying $4A^3 + 27B^2 \neq 0$. Then, there exists a unique lattice $\Lambda \subset \mathbb{C}$ such that*

$$g_2(\Lambda) = 60G_4(\Lambda) = -4A$$

and

$$g_3(\Lambda) = 140G_6(\Lambda) = -4B.$$

The map

$$\mathbb{C}/\Lambda \longrightarrow E : y^2 = x^3 + Ax + B$$

$$z \mapsto (\wp(z;\Lambda), \frac{1}{2}\wp'(z;\Lambda))$$

is a complex analytic isomorphism.

Proof: By the previous theorem, there exists $\tau \in \mathbb{H}$ such that

$$j(\tau) = 1728\frac{4A^3}{4A^3 + 27B^2}.$$

(i) First assume $\underline{AB \neq 0}$. By definition of $j(\tau)$, we get

$$\frac{27B^2}{4A^3} = \frac{1728}{j(\tau)} - 1 = \frac{27g_3(\tau)^2}{g_2(\tau)^3}.$$

So,

$$\left(\frac{B}{g_3(\tau)}\right)^2 \cdot \left(\frac{g_2(\tau)}{A}\right)^3 = -4.$$

Let

$$\alpha = \sqrt{\frac{Ag_3(\tau)}{Bg_2(\tau)}}$$

and $\Lambda = \alpha.\Lambda_\tau = \mathbb{Z}\alpha\tau + \mathbb{Z}\alpha$.

Then,

$$g_2(\Lambda) = \alpha^{-4} g_2(\Lambda_\tau) = \frac{B^2 g_2(\tau)^3}{A^2 g_3(\tau)^2} = -4A,$$

$$g_3(\Lambda) = \alpha^{-6} g_3(\Lambda_\tau) = \frac{B^3 g_2(\tau)^3}{A^3 g_3(\tau)^2} = -4B.$$

(ii) A=0: Then, $j(\tau) = 0$ and $g_2(\tau) = 0$. It is enough to take $\Lambda = \alpha\Lambda_\tau$ with

$$\alpha = \sqrt[6]{\frac{g_3(\tau)}{-4B}}.$$

(iii) B=0: Then, $j(\tau) = 1728$ and $g_3(\tau) = 0$. Similar with case (ii), it is enough to take $\Lambda = \alpha\Lambda_\tau$ where

$$\alpha = \sqrt[4]{\frac{g_2(\tau)}{-4A}}.$$

q-Expansions of Some Modular Functions

As we have seen in the Chapter I, the Eisenstein series $G_{2k}(\tau)$ is a modular function of weight k. It satisfies $G_{2k}(\tau + 1) = G_{2k}(\tau)$, so it has a Fourier expansion in terms of $q = e^{2i\pi\tau}$. Now, we will compute this Fourier series and use it to get Fourier expansions of $\Delta(\tau)$ and $j(\tau)$.

Proposition 3.16 *Let $k \geq 2$. Then*

$$G_{2k}(\tau) = 2\zeta(2k) + 2\frac{(2i\pi)^{2k}}{(2k-1)!} \sum_{n\geq 1} \sigma_{2k-1}(n) q^n,$$

where $\zeta(s) = \sum\limits_{n\geq 1} \frac{1}{n^s}$ is the Riemann ζ-function and $\sigma_k(n) = \sum\limits_{d|n} d^k$ is the k^{th}-power divisor function.

Proof: [6, Chapter I, Section 7]

Proposition 3.17 *The modular j-function has the Fourier expansion*

$$j(\tau) = \frac{1}{q} + \sum_{n\geq 0} c(n) q^n,$$

where $c(n) \in \mathbb{Z}$ for all n.

Proof: [6, Chapter I, Section 7]

Theorem 3.18 (Jacobi)

$$\Delta(\tau) = (2\pi)^{12} q \prod_{n\geq 1} (1 - q^n)^{24}.$$

Proof: [6, Chapter I, Section 8]

CHAPTER 4

Uniformization of Elliptic Curves over $\mathbb{Q}_p$

In the previous chapter we saw that each elliptic curve $\mathbb{C}$ comes from a lattice over $\mathbb{C}$. In this chapter we will answer the question what happens if we change the base field. We will be considering the p-adic field $\mathbb{Q}_p$ and finite extensions K of $\mathbb{Q}_p$. The same question arises: Is there any relation between the set of lattices in K and the set of elliptic curves defined over K?

The first approach would be to use the same argument that we have used for elliptic curves over $\mathbb{C}$. However this directly fails since $\mathbb{Q}_p$ has no nontrivial lattices. Indeed, let Λ be a subgroup in $\mathbb{Q}_p$. Take any $t \in \Lambda$. Then,

$$lim_{n\to\infty} p^n t = 0.$$

So, each nontrivial element of Λ would cause 0 to be an accumulation point. Hence, $\mathbb{Q}_p$ has no nontrivial discrete subgroup.

Tate's idea to avoid this situation is to exponentiate first and then consider lattices. This approach works since $\mathbb{Q}_p^*$ has nontrivial lattices.

More generally, we will be working in a finite extension K of $\mathbb{Q}_p$, which we call a p-adic field.

Theorem 4.1 *Let K be a p-adic field with absolute value $|.|$ and let $\overline{K}$ be the algebraic closure of K. Let $q \in K^*$ with $|q| < 1$ and for every $k \in \mathbb{Z}$ let*

$$s_k(q) = \sum_{n\geq 1} \frac{n^k q^n}{1-q^n},$$

$$a_4(q) = -5s_3(q),$$

$$a_6(q) = -\frac{5s_3(q) + 7s_5(q)}{12}.$$

(a) The series $s_k(q), a_4(q)$ and $a_6(q)$ converge in K.

Define the Tate curve E_q by

$$E_q : y^2 + xy = x^3 + a_4(q)x + a_6(q).$$

(b) *The Tate curve is an elliptic curve over K with discriminant*

$$\Delta = q\prod_{n\geq 1}(1-q^n)^{24}$$

and j-invariant

$$j(E_q) = \frac{1}{q} + \sum_{n\geq 1} c(n)q^n$$

with $c(n) \in \mathbb{Z}$.

(c) *The series*

$$X(u,q) = \sum_{n\in\mathbb{Z}} \frac{q^n u}{(1-q^n u)^2} - 2s_1(q)$$

$$Y(u,q) = \sum_{n\in\mathbb{Z}} \frac{(q^n u)^2}{(1-q^n u)^3} + s_1(q)$$

converge for all $u \in \overline{K}, u \notin q^{\mathbb{Z}}$. They define a surjective homomorphism

$$\phi : \overline{K^*} \longrightarrow E_q(\overline{K})$$

$$u \mapsto \begin{cases} (X(u,q), Y(u,q)) & \text{if} \quad u \notin q^{\mathbb{Z}} \\ 0 & \text{if} \quad u \in q^{\mathbb{Z}} \end{cases}$$

with $ker\phi = q^{\mathbb{Z}}$, where 0 is the base point of the elliptic curve.

(d) *ϕ is compatible with the action of the Galois group $G_{\overline{K}/K}$ in the sense that*

$$\phi(u^\sigma) = \phi(u)^\sigma \text{ for all } u \in \overline{K}^*,\ \sigma \in G_{\overline{K}^*/K}.$$

In particular, for any algebraic extension L/K, ϕ induces an isomorphism:

$$\phi : L^*/q^{\mathbb{Z}} \longrightarrow E_q(L).$$

Proof:

(a) The proof of the convergence of the series $s_k(q)$ follows immediately from the fact:

Let K be a valued field with valuation v. A series $\sum_{n\geq 1} a_n$ with $a_n \in K$ is convergent if and only if $v(a_n) \to \infty$ whenever $n \to \infty$

Write $a_4(q) = -5s_3(q) = -5\sum_{n\geq 1}\frac{n^3 q^n}{1-q^n}$

Denote the valuation corresponding to the absolute value $|.|$ by v_p. Then,

$$v_p(n^3\frac{q^n}{1-q^n}) = v_p(n^3) + v_p(\frac{q^n}{1-q^n}) = 3v_p(n) + nv_p(q) - v_p(1-q^n).$$

We know that $v_p(1-q^n) \leq inf\{v_p(1), v_p(-q^n)\}$ where $v_p(1) = 0$.

As $|q| < 1$, we have $v_p(q) > 1$. Therefore, $v_p(1)$ and $v_p(-q^n)$ have different values. Hence,

$$v_p(1-q^n) = inf\{v_p(1), v_p(-q^n)\} = 0.$$

Therefore, we get:

$$v_p(n^3 \frac{q^n}{1-q^n}) = 3v_p(n) + nv_p(q) - v_p(1-q^n) = 3v_p(n) + nv_p(q).$$

If we let n tend to infinity, we see that $v_p(n^3 \frac{q^n}{1-q^n})$ also tends to infinity, which means the series $a_4(q)$ is convergent.

To see that the series $a_6(q)$ is convergent, first we will show that the coefficients of $a_6(q)$ are in $\mathbb{Z}$, when $a_6(q)$ considered as a power series in q:

$$a_6(q) = -\frac{5s_3(q) + 7s_5(q)}{12} = -\frac{5\sum\limits_{n\geq 1}\sigma_3(q)q^n + 7\sum\limits_{n\geq 1}\sigma_5(q)q^n}{12} = -\frac{\sum\limits_{n\geq 1}[5\sigma_3(q) + 7\sigma_5(q)]}{12}$$

Claim: $5\sigma_3(q) + 7\sigma_5(q) \equiv 0 \bmod 12$

Proof of the Claim:

$$5\sigma_3(q) + 7\sigma_5(q) = 5\sum_{d|q} d^3 + 7\sum_{d|q} d^5 = \sum_{d|q}[5d^3 + 7d^5].$$

Therefore to prove our claim, it is enough to prove that $5d^3 + 7d^5 \equiv 0 \bmod 12$ where $d \in \mathbb{Z}$. As $d \in \mathbb{Z}$, d can be congruent one of 0,1,2,3,4,5,6,7,8,9,10,11 modulo 12. After doing some computation, one can see easily that our claim is true.

(b) Follows by an analogous idea as Jacobi identity. For the complete proof please see [6, Chapter 5, Section 3]

(c) (i) To prove the series $X(u,q)$ is convergent, we need:

Claim: The series $s_1(q)$ is equal to $\sum\limits_{n\geq 1} \frac{q^n}{(1-q^n)^2}$.

Proof of the Claim: To see this equality, first note that

$$\frac{t}{(1-t)^2} = T.\frac{d}{dT}(\frac{1}{1-T}) = T.\frac{d}{dT}\sum_{m\geq 0} T^m = \sum_{m\geq 1} mT^m.$$

Now, substitute $T = q^n$ and sum over $n \geq 1$, and we get

$$\sum_{n\geq 1}\frac{q^n}{(1-q^n)^2} = \sum_{n\geq 1}\sum_{m\geq 1} mq^{nm} = \sum_{m\geq 1} m \sum_{n\geq 1} q^{nm} = \sum_{m\geq 1}\frac{mq^m}{1-q^m},$$

which proves our claim.

Therefore,

$$X(u,q)=\sum_{n\in\mathbb{Z}}\frac{q^nu}{(1-q^nu)^2}-2\sum_{n\geq 1}\frac{q^n}{(1-q^n)^2}.$$

Let us consider the first series in the sum: $\sum\limits_{n\in\mathbb{Z}}\frac{q^nu}{(1-q^nu)^2}$ $(*)$

For $n=0$, the series $(*)$ is $\frac{u}{(1-u)^2}$. Then, we can rewrite the series as

$$\frac{u}{(1-u)^2}+\sum_{n\leq -1}\frac{q^nu}{(1-q^nu)^2}+\sum_{n\geq 1}[\frac{q^nu}{(1-q^nu)^2}-2\frac{q^n}{(1-q^n)^2}].$$

Denote by A the second series $\sum\limits_{n\leq -1}\frac{q^nu}{(1-q^nu)^2}$ in the new sum. By rewriting the index, we can write A as $\sum\limits_{n\geq 1}\frac{q^{-n}u}{(1-q^{-n}u)^2}$. Then,

$$X(u,q)=\frac{u}{(1-u)^2}+\sum_{n\geq 1}[\frac{q^nu}{(1-q^nu)^2}+\frac{q^{-n}u}{(1-q^{-n}u)^2}-2\frac{q^n}{(1-q^n)^2}]$$

Now, multiply the numerator and the denominator of the term of series A by $\frac{q^{2n}}{u^2}$:

$$\frac{q^{-nu}}{(1-q^{-n}u)^2}.\frac{\frac{q^{2n}}{u^2}}{\frac{q^{2n}}{u^2}}=\frac{q^{-n}u.\frac{q^{2n}}{u^2}}{(1-q^{-n}u)^2.\frac{q^{2n}}{u^2}}=\frac{q^nu^{-1}}{((1-q^{-n}u).\frac{q^n}{u})^2}=\frac{q^nu^{-1}}{(\frac{q^n}{u}-1)^2}=\frac{q^nu^{-1}}{(1-q^nu^{-1})^2}.$$

Consider the first term in the sum: $\frac{u}{(1-u)^2}$. Dividing the numerator and denominator of this term by u, we get: $\frac{1}{u+u^{-1}-2}$.

Therefore, the series $X(u,q)$ becomes:

$$\frac{1}{u+u^{-1}-2}+\sum_{n\geq 1}[\frac{q^nu}{(1-q^nu)^2}+\frac{q^nu^{-1}}{(1-q^nu^{-1})^2}-2\frac{q^n}{(1-q^n)^2}].$$

To see that this series is convergent we will use the fact that a series $\sum\limits_{n=m}^{\infty}a_nx^n$ is convergent if and only if $v_p(a_n)\to\infty$ as $n\to\infty$.

Now,

$$v_p\left(\frac{q^nu}{(1-q^n)^2}+\frac{q^nu^{-1}}{(1-q^nu^{-1})^2}-2\frac{q^n}{(1-q^n)^2}\right)\geq min\left\{v_p\left(\frac{q^nu}{(1-q^nu)^2}\right),v_p\left(\frac{q^nu^{-1}}{(1-q^nu^{-1})^2}\right),v_p\left(-2\frac{q^n}{(1-q^n)^2}\right)\right\}.$$

Let us consider the valuations separately.

$$v_p(\frac{q^nu}{(1-q^nu)^2})=v_p(q^n)+v_p(u)-2v_p(1-q^nu).$$

Here since $v_p(1)\neq v_p(q^nu)$, we have $v_p(1-q^nu)=min\{v_p(1),v_p(q^nu)\}=v_p(1)$, which is 0. Hence,

$$v_p(\frac{q^nu}{(1-q^nu)^2})=v_p(q^n)+v_p(u)=nv_p(q)+v_p(u).$$

And,

$$v_p(\frac{q^n u^{-1}}{(1-q^n u^{-1})^2}) = nv_p(q) - v_p(u) - 2v_p(1-q^n u^{-1}).$$

By a similar argument as above, here $v_p(1-q^n u^{-1}) = 0$. Hence,

$$v_p(\frac{q^n u^{-1}}{(1-q^n u^{-1})^2}) = nv_p(q) - v_p(u).$$

Similarly,

$$v_p(\frac{q^n}{(1-q^n)^2}) = v_p(q^n) - 2v_p(1-q^n)^2.$$

The latter one is equal to 0 by the same argument. So,

$$v_p(\frac{q^n}{(1-q^n)^2}) = v_p(q^n) = nv_p(q).$$

Therefore,

$v_p(\frac{q^n u}{(1-q^n)^2} + \frac{q^n u^{-1}}{(1-q^n u^{-1})^2} - 2\frac{q^n}{(1-q^n)^2}) \geq min\{v_p(\frac{q^n u}{(1-q^n u)^2}), v_p(\frac{q^n u^{-1}}{(1-q^n u^{-1})^2}), v_p(-2\frac{q^n}{(1-q^n)^2})\}.$

By the calculations above, the latter one in the inequality is equal to

$$min\{nv_p(q) + v_p(u), nv_p(q) - v_p(u), nv_p(q)\},$$

which tends to infinity as $n \to \infty$.

Therefore, the series $X(u,q)$ is convergent.

Now, let us consider the series $Y(u,q) = \sum_{n\in\mathbb{Z}} \frac{(q^n u)^2}{(1-q^n u)^3}$.

Similar to the above, we can write it as

$$Y(u,q) = \frac{u^2}{(1-u)^3} + \sum_{n\geq 1}[\frac{(q^n u)^2}{(1-q^n u)^3} + \frac{q^n}{(1-q^n)^2}] + \sum_{n\leq -1} \frac{(q^n u)^2}{(1-q^n u)^3}.$$

We can write the latter term in the sum as $\sum_{n\geq 1} \frac{(q^{-n}u)^2}{(1-q^{-n}u)^3}$ by changing the index.

As we did for the series $X(u,q)$, we multiply the numerator and denominator for this series by $\frac{q^{3n}}{u^3}$. Hence we get:

$$\sum_{n\geq 1} \frac{(q^{-n}u)^2}{(1-q^{-n}u)^3} = \sum_{n\geq 1} -\frac{q^n u^{-1}}{(1-q^n u^{-1})^3}.$$

Then, we can write the series $Y(u,q)$ as follows:

$$\frac{u^2}{(1-u)^3} + \sum_{n\geq 1}[\frac{(q^n u)^2}{(1-q^n u)^3} - \frac{q^n u^{-1}}{(1-q^n u^{-1})^3} + \frac{q^n}{(1-q^n)^2}].$$

By a similar calculations as for the series $X(u,q)$, we get

$$v_p(\frac{(q^n u)^2}{(1-q^n u)^3} - \frac{q^n u^{-1}}{(1-q^n u^{-1})^3} + \frac{q^n}{(1-q^n)^2}) \to \infty$$

as n tends to infinity.

Hence $Y(u,q)$ is convergent.

Note that $u \notin K$, but $u \in \overline{K}$. But, $K(u)$ is a finite extension of K, hence complete. All series are in $K(u)[[q]]$, and therefore the series converge to an element in $K(u)$, which is in $\overline{K}$.

Next we prove that ϕ is a homomorphism.

Take any $u_1, u_2 \in \overline{K}^*$. Let $u_3 = u_1u_2$. Denote by P_i the image of u_i under the map ϕ for $i = 1,2,3$, i.e,

$$P_i = \phi(u_i) \text{ for } i = 1,2,3.$$

Our aim is to show that $P_3 = P_1 \oplus P_2$. We prove it case by case.

By the periodicity $\phi(qu) = \phi(u)$, it is enough to consider u_1, u_2 in the ranges $|q| < |u_1| \leq 1$ and $1 \leq |u_2| \leq |q|^{-1}$, which gives us $|q| < |u_3| < |q|^{-1}$

(i) First assume that $u_1 = 0$. Then by definition of ϕ, $P_1 = \phi(u_1) = 0$. So,

$$P_3 = (X(u_2,q), Y(u_2,q) = P_2 + 0 = P_2 + P_1.$$

Hence, ϕ is a homomorphism if $u_1 = 0$. Since the situation is symmetric, same argument hold if $u_2 = 0$. So, we have proved our claim if $u_1 = 0$ or $u_2 = 0$.

(ii) Now, let us assume $u_1u_2 = 1$. Then, $u_2 = u_1^{-1}$. So,

$$P_3 = \phi(u_3) = (X(u_1u_2,q), Y(u_1u_2,q)) = \phi(1) = 0.$$

Claim: $P_1 \oplus P_2 = 0$ if and only if $X(u_1,q) = X(u_2,q)$ and $Y(u_1,q) + Y(u_2,q) = -X(u_1,q)$

Proof of the Claim: Claim follows from the identities

$X(u^{-1},q) = X(u,q)$ and $Y(u^{-1},q) = -Y(u,q) - X(u,q)$

Now, as $u_1u_2 = 1$, $u_2 = u_1^{-1}$. So, by using the identities for the series $X(u,q)$ and $Y(u,q)$, we get directly $P_1 \oplus P_2 = 0$.

Therefore, we are in the case that P_1, P_2, P_3 are all different from 0.

Write $P_i = (x_i, y_i)$ where $x_i = X(u_i,q)$, $y_i = Y(u_i,q)$ for $i = 1,2,3$.

(iii) Assume $x_1 \neq x_2$. By the group law on E_q, we have

$$x_3 = \lambda^2 + a_1\lambda - a_2 - x_1 - x_2$$

where $\lambda = \frac{y_2 - y_1}{x_2 - x_1}$.

$$\Rightarrow x^3(x_2 - x_1)^2 = (y_2 - y_1)^2 + (y_2 - y_1)(x_2 - x_1) - (x_1 + x_2)(x_2 - x_1)^2$$

Similarly, we get

$$y_3 = -(\lambda + a_1)x_3 - \nu - a_3$$

where $\nu = \frac{y_1x_2 - y_2x_1}{x_2 - x_1}$.

$$\Rightarrow y_3(x_2 - x_1) = x_3(y_1 - y_2 + x_2 - x_1) - (y_1x_2 - y_2x_1).$$

We know that if we substitute for these any complex numbers u_1, u_2, q in the ranges that we considered at the beginning of the proof of part (c), these identities still hold. Hence they are identities in the ring $\mathbb{Q}(u_1, u_2)[[q]]$, the ring of formal power series in q with coeffiecients that are rational functions of u_1, u_2. So they are true for $u_1, u_2, q \in \overline{K}$.

(iv) Suppose that $x_1 = x_2$. Note that $x_1 = x_2$ if and only if $P_1 = \bigoplus P_2$

We need:

Lemma 4.2 *Let ϕ be a map of a multiplicative group into an additive group which takes on an infinite number of distinct values and satisfies*

$$\phi(u_1u_2) = \phi(u_1) + \phi(u_2) \textit{ whenever } \phi(u_1) \neq \pm\phi(u_2)$$

Then, ϕ is a homomorphism.

Proof: [6, Chapter V, Section 3]

By the lemma, to finish the proof we need to show that ϕ takes on infinitely many distinct values:

The series for $X(u, q)$ shows that for any $t \in K$ with $|t| < 1$, we have

$$|X(t + 1, q)| = |t|^{-1}.$$

Therefore, by lemma 3.2, ϕ is a homomorphism.

The only thing remaining is to show that ϕ is surjective.

Let f be a meromorphic elliptic function, i.e, $f = \frac{g}{h}$ where g, h are holomorphic functions and f satisfies $f(z) = f(qz)$. Let us consider the zeros of the functions g and h. As $f(z) = f(qz)$ and the zeros of g gives us the zeros of f, zeros of g are invariant under multiplication by q. The same is true for h, zeros of h are invariant under multiplication by q. Let us consider the functions $g(t)$ and $g(qt)$. Since zeros of g are invariant under multiplication by q, zeros of these two functions are the same. By Schnirelmann, g satisfies $g(t) = ct^ng(qt)$ for some $t \in \mathbb{Z}$ and for some constant c. By similar as above, $h(t) = dt^mh(qt)$ where $m \in \mathbb{Z}$ and d constant. Since, $f = \frac{g}{h}$ and $f(t) = f(qt)$, we get that $c = d$ and $n = m$, otherwise $\frac{g}{h}$ is not invariant under multiplication by q. Such functions are called *theta functions of type ct^n* and n is called *the order of the theta function*. So, g and h are theta functions of type ct^n of order n. Hence, we see that a meromorphic function can be written as a fraction of two theta functions of the same order. Consider the Laurent series of the function g. Since $g(t) = ct^ng(qt)$, the Newton polygon of g is invariant under the map $(x, y) \mapsto (x + n, y - log|c| - xlog|q|)$. Hence, we see that g has n roots in the annulus $r|q| < |t| < |r|$. Similarly, as g and h are theta functions of the same type h also has n roots in the same annulus.

Now we are ready to prove that ϕ is surjective.

Take any $(x_0, y_0) \in E_q$. Consider the map $\psi : \overline{K}^*/q^{\mathbb{Z}} \to E_q$ which is defined by $u \mapsto \psi(u) = X(u, q) - x_0$. By the definition of $X(u, q)$, the map ψ has a pole in $q^{\mathbb{Z}}$. Then, by the discussion above ψ also has a root, i.e, $X(u_0, q) - x_0 = 0$ for some $u_0 \in \overline{K}^*/q^{\mathbb{Z}}$, which implies that there exists $u_0 \in \overline{K}^*/q^{\mathbb{Z}}$ such that $x_0 = X(u_0, q)$.

Now, if we consider $Y(u_0, q)$, then $Y(u_0, q) = y_0$ or $Y(u_0, q) = -y_0$. If necessary, by taking $\frac{1}{u_0}$, we can say that $Y(u_0, q) = y_0$.

Therefore, ϕ is surjective.

(d) The series $X(u, q)$ and $Y(u, q)$ are convergent in the complete field $K(u)$ as explained above. So, it suffices to prove the claim for $\sigma \in G_{L/K}$, where L is a finite Galois extension of K containing $K(u)$.

Take any $\sigma \in G_{L/K}$. Denote by $\mathcal{P}$, the maximal ideal of the valuation ring of L. Then, $\sigma(\mathcal{P}) = \mathcal{P}$. Hence,

$$|\alpha^\sigma| = |\alpha|$$

for all $\sigma \in G_{L/K}$ and $\alpha \in L$.

Claim: If $\sum \alpha_i$ is a convergent series with $\alpha_i \in L$ and $\sum \alpha_i = \alpha$, then

$$(\sum \alpha_i)^\sigma = \sum (\alpha_i)^\sigma.$$

Proof of the Claim: As

$$|\alpha_1^\sigma + \cdots + \alpha_n^\sigma - \alpha^\sigma| = |(\alpha_1 + \cdots + \alpha_n - \alpha)^\sigma| = |\alpha_1 + \cdots + \alpha_n - \alpha|,$$

we are done.

Bibliography

[1] F. Bruhat, *Lectures on Some Aspects of p-Adic Analysis*, Tata Institute of Fundamental Research, 1963

[2] A.J. Engler, A. Prestel, *Valued Fields*, Springer Monographs in Mathematics, Springer-Verlag, Berlin, Heidelberg, 2005

[3] B. Dwork, G. Gerotto, F.J. Sullivan, *An Introduction to G-Functions*, Annals of Math. Studies 133, Princeton University Press, 1994

[4] A. Robert, *Elliptic Curves*, Lecture Notes in Mathematics 326, Berlin, New York, Springer-Verlag, 1973

[5] J.H. Silverman, *The Arithmetic of Elliptic Curves*, Graduate Texts in Mathematics 106, Springer-Verlag, New York, 1986

[6] J.H. Silverman, *Advanced Topics in the Arithmetic of Elliptic Curves*, Graduate Texts in Mathematics 151, Springer-Verlag, 1994

[7] J.Tate, *A Review of Non-Archimedean Elliptic Functions*, in Coates, John; Yau, Shing-Tung, Elliptic Curves, modular forms and Fermat's last theorem(Hong Kong, 1993), Series in Number Theory I, Int. Press, Cambridge, MA, pp 162-184.