UNIVERSITÀ
DEGLI STUDI
DI PADOVA

Università degli Studi di Padova

DIPARTIMENTO DI MATEMATICA "TULLIO LEVI-CIVITA"

Corso di Laurea Triennale in Matematica

P-adic Uniformisation of elliptic curves

Relatore:
Prof. Matteo Longo

Laureando: Francesco Tonon
Matricola: 2020600

Anno Accademico 2023/2024

19/07/2024

Contents

Chapter 1

Elliptic Curves

1.1 Weierstrass equation

In this first chapter, we define elliptic curves, and we state some of their properties.

Definition 1.1.1. An elliptic curve is a pair (E, O) where E is a non-singular projective curve of genus one over a field K and a point $O \in E$.

For arithmetic purposes, it is more natural to work with explicit equations, as explained in the following theorem.

Theorem 1.1.2. *Let (E, O) be an elliptic curve defined on K.*

1. *There exist constants a_1, a_2, a_3, a_4, a_6 and an isomorphism given by the map:*

$$\phi : E \xrightarrow{\cong} \{[X, Y, \mathbb{Z}] \in \mathbb{P}^2_K : [X, Y, Z] \in \text{ curve given by } C \subset \mathbb{P}^2_{\mathbb{K}}\} \tag{1.1}$$

   where

$$C : Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3 \tag{1.2}$$

   which is the Weierstrass equation for C and $\phi(O) = [0, 1, 0]$.

2. *For both of the two Weierstrass equations, that describes the same curve E, there exists a linear change of variable that fixes O*

$$Y = u^2X' + r, \qquad Y = u^3Y' + su^2X' + t \tag{1.3}$$

   with $u \in K^*$ and $r, s, t \in K$.

3. *Conversely, every smooth cubic projective curve C given by a Weierstrass equation is an elliptic curve on K with base point $O = [0, 1, 0]$.*

This theorem is proven using the Riemann-Roch Theorem and some basic knowledge about maps between algebraic curves; a more complete proof is given in [8, Chapter III]. Weierstrass equation can be simplified, if we consider the base point $O = [0 : 1 : 0]$. Then

we dehomogenise it to obtain the elliptic curve in nonhomogeneous coordinates $x = X/Z$ and $y = Y/Z$ in the affine space $U_Z = \{[x : y : 1] : (x, y) \in \mathbb{C}^2\}$:

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \tag{1.4}$$

where we need to keep in mind that O is not in $E \cap \mathbb{A}^2_K$. We now study fields K that have $char(K) = 0$; this includes $\mathbb{C}$ and the p-adic fields, in which we will be most interested.

Definition 1.1.3. Suppose E/K is an elliptic curve given by the general formula

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \tag{1.5}$$

So, we define some quantities related to elliptic curves. Then, we simplify the equation of elliptic curves by completing the square with the following map:

$$y \mapsto \frac{1}{2}(y - a_1x - a_3) \tag{1.6}$$

$$b_2 = a_1^2 + 4a_2, \qquad b_4 = 2a_4 + a_1a_3, \qquad b_6 = a_3^2 + 4a_6, \tag{1.7}$$

which gives us the simplified equation

$$y^2 = 4x^3 + b_2x^2 + 2b_4x + b_6. \tag{1.8}$$

We also develop more quantities which help us write the invariants of elliptic curves

$$b_8 = a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2, \tag{1.9}$$

$$c_4 = b_2^2 - 24b_4 \tag{1.10}$$

$$c_6 = -b_2^3 + 36b_2b_4 - 216b_6. \tag{1.11}$$

Let us define: the discriminant of an elliptic curve E that is

$$\Delta(E) = -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b2b_4b_6 \tag{1.12}$$

the j-invariant for E is

$$j(E) = c_4^3/\Delta \tag{1.13}$$

the Hasse invariant of E to be

$$\gamma(E/K) = -c_4/c_6 \tag{1.14}$$

and the differential

$$\omega = \frac{\mathrm{d}x}{2y + a_1x + a_3}. \tag{1.15}$$

Additionally, if $char(K) \neq 2, 3$, we can further simplify by completing the cube with the map

$$(x, y) \mapsto \left(\frac{x - 3b_2}{36}, \frac{y}{108}\right). \tag{1.16}$$

We obtain the equation

$$E : y^2+ = x^3 + Ax + B. \tag{1.17}$$

Those quantities are all well-defined, and they have some properties which we can now analyse.

Theorem 1.1.4. *The curve E given in the Weierstrass equation over a field K is nonsingular, if for every point $P \in K$ at least one of the following is not equal to* 0*:*

$$\frac{\partial f}{\partial x}(P), \frac{\partial f}{\partial y}(P) \tag{1.18}$$

where

$$f(x, y) = y^2 + a_1xy + a_3y^2 - (x^3 + a_2x^2 + a_4x^2 + a_6). \tag{1.19}$$

1. *An elliptic curve given in the Weierstrass equation satisfies one of the following:*
   (a) *it is nonsingular if and only if $\Delta \neq 0$;*
   (b) *it has a node if and only if $\Delta = 0$ and $c_4 \neq 0$;*
   (c) *it has a cusp if and only if $\Delta = c_4 = 0$.*

   In cases 1b and 1c, there is only one singular point.
2. *Two elliptic curves are isomorphic over $\overline{K}$ if and only if they have the same j-invariant.*
3. *Let $j_0 \in \overline{K}$. There exists an elliptic curve defined over $K(j_0)$ whose j-invariant is equal to j_0.*

Proof. We prove 1 by showing that the point at infinity, which is $O = [0, 1, 0]$, is never singular. This is true as $\frac{\partial F}{\partial Z}(O) = 1 \neq 0$.
Next, suppose that E is singular, say at $P_0 = (x_0, y_0)$.
The substitution $x = x + x_0,\ y = y + y_0$ leaves Δ and c_4 invariant, so we assume that E is singular at $(0, 0)$. Then,

$$a_6 = -f(0, 0) = 0, a_4 = -\frac{\partial f}{dx}(0, 0) = 0, a_3 = \frac{\partial f}{dy}(0, 0) = 0, \tag{1.20}$$

so the equation for E takes the form

$$E : f(x, y) = y^2 + a_1xy - a_2x^2 - x^3 = 0. \tag{1.21}$$

This equation has associated quantities

$$c_4 = (a_1^2 + 4a_2)^2 \text{ and } \Delta = 0. \tag{1.22}$$

By definition, E has a node, respectively cusp, at $(0, 0)$ if the quadratic form $y^2+a_1xy-a_2x^2$ has distinct, respectively equal, factors, which occurs if and only if the discriminant of this quadratic form satisfies

$$a_1^2 + 4a_2 \neq 0, \text{ respectively } a_1^2 + 4a_2 = 0. \tag{1.23}$$

This completes the proof of 1c,1b. In order to complete the proof of 1 it remains to show the case with E is non singular, implies $\Delta \neq 0$.

To simplify the computation, we assume that $char(K) \neq 2$ and consider a Weierstrass equation of the form

$$E : y^2 = 4x^3 + b_2x^2 + 2b_4x + b_6. \tag{1.24}$$

The curve E is singular if and only if there is a point $(x_0, y_0) \in E$ that satisfies equations $2y_0 = 0$ and $12x^2 + 2b_2x_0 + 2b_4 = 0$. To put it differently, the singular points correspond exactly to the coordinates (x_0, y_0) where x_0 is a double root of the cubic polynomial:

$$4x^3 + b_2x^2 + 2b_4x + b_6. \tag{1.25}$$

This polynomial has a double root if and only if its discriminant is zero.
We now prove 2.
If E_1 and E_2 are isomorphic than by the formulas they have the same j-invariant. On the other hand, if they have the same j-invariant and, for semplicity assume $char(K) \geq 5$, we can find the following relation:

$$j(E_1) = \frac{4A_1^3}{4A_1^3 + 27B_1^2} = \frac{4A_2^3}{4A_2^3 + 27B_2^2} = j(E_2). \tag{1.26}$$

This leads us to consider the relation $A_1^3B_2^2 = A_2^3B_1^2$. We consider here only the general case where $j \neq 0, 1728$ and we are able to find a change of variable as follows:

$$(x, y) = (u^2x', u^3y') \tag{1.27}$$

$$\text{where } u = (A_1/A_2)^{1/4}. \tag{1.28}$$

To prove 3, we give the curve

$$E : y^2 + xy = x^3 - \frac{36}{j_0 - 1728}x - \frac{1}{j_0 - 1728}, \tag{1.29}$$

which gives us the desired result if $j \neq 0, 1728$, and the other cases are trivial. □

1.2 Group law and maps

We now define the sum of points on an elliptic curve.

Definition 1.2.1. For every $P, Q \in E/K$ we define the operation of composition of points on the elliptic curve $\oplus : E \times E \to E$ and let $P, Q, R \in E$ and O as usual. We define $P \oplus Q$ as the point we obtain with the following algorithm: we take the line through P, Q $L = L(P, Q)$ so we find $R = L \cap E$ the third intersection. Then $L' = L(R, O)$ gives us the third point $-R = L' \cap E$, which we define $P \oplus Q$. So, we now understand that E with composition $\oplus$ is an abelian group with identity O.

Theorem 1.2.2. *Let E be an elliptic curve with Weierstrass equation:*

$$y^2 + a_1xy + a_3y^2 = (x^3 + a_2x^2 + a_4x^2 + a_6). \tag{1.30}$$

.

1. *Let $P_0 = (x_0, y_0)$, then*
$$-P_0 = (x_0, -y_0 - a_1 x_0 - a_3). \tag{1.31}$$
Next, let
$$P_1 + P_2 = P_3 \qquad \text{with} \qquad P_1 = (x_i, y_i) \in E \ \text{ for } i = 1, 2, 3. \tag{1.32}$$

2. *If $x_1 = x_2$ and $y_1 + y_2 + a_1 x_2 + a_3 = 0$, then*
$$P_1 + P_2 = O. \tag{1.33}$$
Otherwise, we define λ, ν by the following formulas:

	λ	ν
$x_1 \neq x_2$	$\frac{y_2 - y_1}{x_2 - x_1}$	$\frac{y_1 x_2 - y_2 x_1}{x_2 - x_1}$
$x_1 = x_2$	$\frac{3x_1^2 + 2a_2 x_1 + a_4 - a_1 y_1}{2y_1 + a_1 x_1 + a_3}$	$\frac{-x_1^3 + a_2 x_1^2 + 2a_6 - a_3 y_1}{2y_1 + a_1 x_1 + a_3}$

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

3. *With notation as above, $P_1 + P_2 = P_3$ has coordinates:*
$$x_3 = \lambda^2 + a_1 \lambda - a_2 - x_1 - x_2, \tag{1.34}$$
$$y_3 = -(\lambda + a_1) \cdot x_3 - \nu - a_3. \tag{1.35}$$

4. *If $P_1 \neq \pm P_2$.*
$$x(P_1 + P_2) = \left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 + a_1 \left(\frac{y_2 - y_1}{x_2 - x_1}\right) - a_2 - x_1 - x_2, \tag{1.36}$$
and the duplication formula for $P = (x, y) \in E$:
$$x([2]P) = \frac{x^4 - b_4 x^2 - 2b_6 x - b_8}{4x^3 + b_2 x^2 + 2b_4 x + b_6}, \tag{1.37}$$
Here, the coefficients are the same as in 1.1.3.

This theorem is proven in [8, Group law algorithm III.2.3]

Lemma 1.2.3. *Let E be a curve given by a Weierstrass equation with $\Delta = 0$, so E has a singular point S. Then, the composition law makes E_{ns}, the set of non-singular points of E into an abelian group.*

1. *Suppose that E has a node, so $c_4 = 0$, and let*
$$y = \alpha_1 x + \beta_1 \text{ and } y = \alpha_2 x + \beta_2 \tag{1.38}$$
be the distinct tangent lines to E at S. Then, the map
$$E_{ns} \mapsto \overline{K}^*, \qquad (x, y) \mapsto \frac{y - \alpha_1 x - \beta_1}{y - \alpha_2 x - \beta_2} \tag{1.39}$$
is an isomorphism of abelian groups.

2. *Suppose that E has a cusp, so $c_4 = 0$, and let $y = \alpha x + \beta$ be the tangent line to E at S. Thus, the map*

$$E_{ns} \mapsto \overline{K}^{+}, \qquad (x, y) \mapsto \frac{x - x(S)}{y - \alpha x - \beta} \tag{1.40}$$

is an isomorphism of abelian groups.

The proof is given in [8, Theorem III.2.3] In the settings of fields of $char(K) = 0$, the discriminant of the Weierstrass equation is $\Delta = 27A^3 + 27B^2$. Then we study the morphisms between the elliptic curves.

Definition 1.2.4. Let E_1, E_2 be elliptic curves over K. An isogeny ϕ is a morphism $\phi : E_1 \mapsto E_2$ and $\phi(O) = O$. If an isogeny exists with $\phi(E_1) = E_2$ then E_1 and E_2 are said to be *isogenous* otherwise we can show that $\phi(E_1) = O$.

An example of an isogeny is *multiplication-by-m isogeny*. For $m \in \mathbb{Z}$

$$[m] : E \mapsto E. \tag{1.41}$$

If $m > 0$ we define the map as $[m](P) = P + P + P \ldots P$ m times. This map is also defined for negative numbers

$$[m](P) = [-m](-P). \tag{1.42}$$

Theorem 1.2.5. *Let E/K and $m \in \mathbb{Z}^*$, then*

$$[m] : E \mapsto E \tag{1.43}$$

is non constant.

Theorem 1.2.6. *Let E be an elliptic curve and let $\ll \in \mathbb{Z}$ be a prime. The (l-adic) Tate module of E is the group $T_l(E) = \varprojlim_n E[l^n]$, where the inverse limit is taken with respect to the maps $[l]$:*

$$E[l^{n+1}] \xrightarrow{[l]} E[l^n]. \tag{1.44}$$

Where formally, the inverse limit $\varprojlim_n E[l^n]$ consists of all sequences $(a_n)_{n\in\mathbb{N}}$ with the characteristic $a_n \in E[l^n]$. These sequences are compatible with the maps $[l]$, which means that $[l](a_{n+1}) = a_n$ for all $n \in \mathbb{N}$. In other words, each element in the inverse limit is an infinite sequence of elements from each $E[l^n]$ that respects the given structure of the maps.

1.3 Formal group

It is necessary to define the Formal Group since it is essential for the analysis of elliptic curves over Local Fields, as it will come up with a reduction of elliptic curves. We study this because we want to investigate the structure of E near O, which we decide as a new origin and therefore make a change of variable as follows:

$$z = -\frac{x}{y}, \quad w = -\frac{1}{y}. \tag{1.45}$$

Let us give a formal definition of formal groups.

Definition 1.3.1. Let R be a ring; we define a formal group $\mathfrak{F}$ over R as a power series $F(X, Y) \in R[[X, Y]]$ where the following are true:

1. $F(X, Y) = X + Y +$ (terms of degree ≥ 2);
2. $F(X, F(Y, Z)) = F(F(X, Y), Z)$;
3. $F(X, Y) = F(Y, X)$;
4. There is a unique power series $i(T) \in R[[T]]$ such that $F(T, i(T)) = 0$;
5. $F(X, 0) = X$.

We call $F(X, Y)$ the formal group law on $\mathfrak{F}$.

Let E be an elliptic curve over a field K. The formal group associated with E is a formal group law F over K. We denote it by $\hat{E}$, and it is given by a power series. Specifically, there exists a formal group law $F(T_1, T_2)$ over K such that the addition of points on the elliptic curve can be expressed in terms of this formal group law. It is given by the formula:

$$F(z_1, z_2) = z_1 + z + 2 - a_1 z_1 z_2 - a_2(z_1^2 z_2 + z_1 z_2^2) + \cdots \in \mathbb{Z}[a_1, \ldots, a_6][[z_1, z_2]]. \tag{1.46}$$

For a more in detail analysis with also reference to Hensel's lemma are given in [8, p. IV] or [3].

Chapter 2

Elliptic curves over the complex numbers and complex uniformisation

2.1 Elliptic curves over the complex numbers

We now consider elliptic curves over $\mathbb{C}$ as the complex numbers provide an example of a complete field where we uniformise elliptic curves over the field. The theorem of complex uniformisation of elliptic curves states that we can parameterise elliptic curves by quotients of lattices. We start this chapter with definitions of lattices and elliptic functions; the meaning of this might not be clear immediately. For a brief historical account of the elliptic integral, see [9].

Definition 2.1.1. A lattice $\Lambda \subset \mathbb{C}$ is a discrete subgroup. We can define lattices with the equation

$$\Lambda = \{a_1 v_1 + a_2 v_2, a_i \in \mathbb{Z}\}, \tag{2.1}$$

where $\{v_1, v_2\}$ is a base for $\mathbb{R}^2$.

Definition 2.1.2. Let $\Lambda \subset \mathbb{C}$ be a lattice. An elliptic function related to Λ is a meromorphic function $f(z)$ on $\mathbb{C}$ such that

$$f(z + \omega) = f(z) \,\forall\, z \in \mathbb{C} \text{ and } \omega \in \Lambda. \tag{2.2}$$

A function f is meromorphic on an open subset U if it is holomorphic on U except at a finite number of isolated points $z_k \subset U$, which are termed the poles of f. The set of all elliptic functions, related to a specific lattice Λ, is $\mathbb{C}(\Lambda)$.

Remark 2.1.3. Let Λ be a lattice. The fundamental parallelogram of the lattice is a set

$$D = \{a + t\omega_1 + k\omega_2 : (t, k) \in [0; 1[^2\} \text{ where } \omega_1, \omega_2 \text{is a basis of } \Lambda. \tag{2.3}$$

Λ is homotetic to the normalised lattice $\{1, \tau\}$; the exact relation between those two lattices is explain and proven in detail in [7, Chapter I.1].

We say that the order of an elliptic function f is the number of poles, counted with multiplicity in a fundamental lattice D.

Remark 2.1.4. In our investigation of elliptic functions, the simplest nonconstant elliptic function we can define is the Weierstrass $\wp$ function, as each non-constant elliptic function must have at least order 2. In this way, let us also analyse the complete structure of $\mathbb{C}(\Lambda)$.

Definition 2.1.5. Given $\Lambda \subset \mathbb{C}$, the Weierstrass $\wp$-function is defined by the following series:

$$\wp(z;\Lambda) := \frac{1}{z^2} + \sum_{\omega\in\Lambda\setminus\{0\}} \left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2}\right) \tag{2.4}$$

We additionally describe the Eisenstein series of weight $2k$ (for Λ) as the series:

$$G_{2k}(\Lambda) = \sum_{\substack{\omega\in\Lambda\\ \omega\neq 0}} \omega^{-2k}. \tag{2.5}$$

The function $\wp$ is well defined on $\mathbb{C}/\Lambda$. It is established that $\wp'$ is another elliptic function. Consequently, we will examine the characteristics of these functions in the ensuing result, attributed to Weierstrass.

Theorem 2.1.6. *Let $\Lambda \subset \mathbb{C}$ be a lattice.*

1. *The Eisenstein series $G_{2k}(\Lambda)$ converge absolutely $\forall k > 1$.*
2. *The series defining the Weierstrass $\wp$-function converges absolutely and uniformly on every compact subset of $\mathbb{C} \setminus \Lambda$. The series defines a meromorphic function on $\mathbb{C}$ having a double pole with residue 0 at each lattice point and no other poles.*
3. *The Weierstrass $\wp$-function is an even elliptic function.*

Proof. 1. Since Λ is discrete in $\mathbb{C}$, we can find a constant c such that the cardinality of the following set is bounded:

$$\#\{\omega \in \Lambda : N \leq |\omega| < N+1\} < cN.\ \forall N \geq 1. \tag{2.6}$$

We substitute it into the Eisenstein series to obtain

$$\sum_{\substack{\omega\in\Lambda\\ |\omega|\geq 1}} \frac{1}{|\omega|^{2k}} \leq \sum_{N=1}^{\infty} \frac{\#\{\omega \in \Lambda : N \leq |\omega| < N+1\}}{N^{2k}} < \sum_{N=1}^{\infty} \frac{c}{N^{2k-1}} < \infty. \tag{2.7}$$

Therefore, $G_{2k}(\Lambda)$ converge absolutely.

2. If $|\omega| > 2|z|$, then

$$\left|\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2}\right| = \left|\frac{z(2\omega - z)}{\omega^2(z-\omega)^2}\right| \leq \frac{|z(2|\omega| + |z|)}{|\omega|^2(|\omega| - |z|)^2} \leq \frac{10|z|}{|\omega|^2}. \tag{2.8}$$

Then, $\wp(z)$ is absolutely convergent for all $z \in \mathbb{C} \setminus \Lambda$ as in 1. Therefore, $\wp$ is a holomorphic function on $\mathbb{C} \setminus \Lambda$, which has a double pole with residue 0 at each point in Λ.

3. As $\wp$ is uniformly convergent, we can compute its derivative

$$\wp'(z) = -2\sum_{\omega\in\Lambda}\frac{1}{(z-\omega)^3}. \tag{2.9}$$

It follows that, $\wp'$ is an elliptic function as $\wp'(z+\omega) = \wp'(z)$ for all $\omega \in \Lambda$. We integrate it to find:

$$\wp(z+\omega) = \wp(z) + c \ \forall z \in \mathbb{C}, \tag{2.10}$$

where c as in 1, it is independent of z; therefore, if $z = -\frac{1}{2}\omega$, $c = 0$ so $\wp$ is even.

This concludes the proof of the theorem. □

Theorem 2.1.7. *Let $\Lambda \subset \mathbb{C}$ be a lattice. Then*

$$\mathbb{C}(\Lambda) = \mathbb{C}(\wp(z), \wp'(z)), \tag{2.11}$$

which means that every elliptic function is a rational combination of $\wp$ and its derivative $\wp'$.

It is proven directly by showing that they share the same poles and zeros. For a complete proof have a look at [4, Theorem I.3] or [8, Chapter 6.2-3]. At this point, to establish the fundamental algebraic connection between elliptic functions and elliptic curves, we examine the Laurent series expansion of $\wp$ near zero.

Theorem 2.1.8. *The expansion of $\wp$ lets us find the followings:*

1. *The Laurent series for $\wp(z)$ around $z = 0$ is given by*

$$\wp(z) = \frac{1}{z^2} + \sum_{k=1}^{\infty}(2k+1)G_{2k+2}z^{2k}. \tag{2.12}$$

2. *For all $z \in \mathbb{C} \setminus \Lambda$, $\wp$ and $\wp'$ satisfies*

$$\wp'(z)^2 = 4\wp(z)^3 - 60G_4(\Lambda)\wp(z) - 140G_6(\Lambda) \tag{2.13}$$

Proof. We start by proving 1. We study $\wp$ near 0, therefore we consider only $|z| < |\omega|$ in order to obtain

$$\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} = \frac{1}{\omega^2}\left(\frac{1}{(1-z/\omega)^2} - 1\right) = \sum_{n=1}^{\infty}(n+1)\frac{z^n}{\omega^{n+2}} \tag{2.14}$$

By setting $2k = n$ and by substituting $\wp$ we obtain

$$\wp(z) = \frac{1}{z^2} + \sum_{\substack{\omega\in\Lambda\\ |\omega|\neq 0}}\sum_{n=1}^{\infty}(n+1)\frac{z^n}{\omega^{n+2}} = \frac{1}{z^2} + \sum_{k=1}^{\infty}(2k+1)z^{2k}\sum_{\substack{\omega\in\Lambda\\ |\omega|\neq 0}}\omega^{-2(k+1)} \tag{2.15}$$

To prove 2. For the algebraic equation, given the coefficients of the Laurent series of $\wp'^2(z)$, $\wp(z)^3$, $\wp(z)$, we see that

$$f(z) = \wp'(z)^2 - 4\wp(z)^3 + 60G_4\wp(z) + 140G_6 \tag{2.16}$$

is holomorphic at $z = 0$ and it satisfies $f(0) = 0$. So $f(z)$ is constant and identically zero. □

In order to simplify the notation of the relation 2.13, we write

$$g_2 = g_2(\Lambda) = 60G_4(\Lambda) \text{ and } g_3 = g_3(\Lambda) = 140G_6(\Lambda). \tag{2.17}$$

So, the equation of $\wp'(z)$ and $\wp(z)$ becomes

$$\wp'(z)^2 = 4\wp(z)^3 - g_2\wp(z) - g_3. \tag{2.18}$$

We give an isomorphism of complex Lie groups, which are complex analytic manifolds that are also groups.

Theorem 2.1.9. *Let g_2 and g_3 of $\Lambda \subset \mathbb{C}$ be as before.*

1. *The polynomial*
$$f(x) = 4x^3 - g_2x - g_3 \tag{2.19}$$
has distinct roots, so its discriminant $\Delta(f) = g_2^3 - 27g_3^2$ is nonzero.

2. *Let $E/\mathbb{C}$ be the curve*
$$E : y^2 = 4x^3 - g_2x - g_3, \tag{2.20}$$
which from 1 is an elliptic curve. Then, the map
$$\psi : \mathbb{C}/\Lambda \mapsto E(\mathbb{C}) \subset \mathbb{P}^2(\mathbb{C}) \tag{2.21}$$
$$z \mapsto [\wp(z), \wp'(z), 1] \tag{2.22}$$
is a complex analytic isomorphism of complex Lie groups.

The proof is given in [8, Chapter IV.3]

2.2 Complex uniformisation of elliptic curves

We want to state the uniformisation theorem for elliptic curves which says that every elliptic curve over $\mathbb{C}$ is parametrised by elliptic functions. The proof is lengthy and requires more notions about modular functions.

Theorem 2.2.1. *Let $A, B \in \mathbb{C}$ be complex numbers that satisfy $A^3 - 27B^2 = 0$. Then there exists a unique lattice $\Lambda \subset \mathbb{C}$ satisfying $g_2(\Lambda) = A$ and $g_3(\Lambda) = B$.*

The proof of this theorem is given in different forms in other books. An analytic approach is given in [5, Theorem I.3.13] or a proof with modular functions in [7, Theorem I.4.3].

Theorem 2.2.2. *Theorem(Complex uniformisation) Let $E/\mathbb{C}$ be an elliptic curve. There exists a lattice $\Lambda \subset \mathbb{C}$, unique up to homothety, and a complex analytic isomorphism of complex Lie groups:*

$$\psi : \mathbb{C}/\Lambda \mapsto E(\mathbb{C}), \tag{2.23}$$

$$\psi(z) = [\wp(z, \Lambda), \wp'(z, \Lambda), 1]. \tag{2.24}$$

[8, Theorem V.1.1] We can also describe kind of the inverse map of the previous theorem.

Theorem 2.2.3. *Let $E/\mathbb{C}$ be an elliptic curve with Weierstrass coordinate functions x, y. Let Λ be a lattice generated by ω_1, ω_2.*
The map

$$F : E(\mathbb{C}) \longmapsto \mathbb{C}/\Lambda, \qquad F(P) = \int_O^P \frac{dx}{y} \pmod{\Lambda} \tag{2.25}$$

is a complex analytic isomorphism of Lie groups and it is the inverse of 2.24.

We can now see that there is a profound similarity between lattices and elliptic curves. We want to study maps between lattices. If Λ_1 and Λ_2 are lattices in $\mathbb{C}$, and we assume that $\exists \alpha \in \mathbb{C}$ has property $\alpha\Lambda_1 \subset \Lambda_2$. Then, the scalar multiplication by α induces a well-defined holomorphic homomorphism

$$\psi_\alpha : \mathbb{C}/\Lambda_1 \mapsto \mathbb{C}/\Lambda_2, \tag{2.26}$$

$$\psi_\alpha(z) = \alpha * z \mod \Lambda_2. \tag{2.27}$$

We now show that these are essentially the only holomorphic maps from $\mathbb{C}/\Lambda_1$ to $\mathbb{C}/\Lambda_2$.

Theorem 2.2.4. *1. With the notation as above, the map*

$$\{\alpha \in \mathbb{C} : \alpha\Lambda_1 \subset \Lambda_2\} \mapsto \{ \textit{maps } \psi : \mathbb{C}/\Lambda_1 \mapsto \mathbb{C}/\Lambda_2 \textit{ and } \psi(0) = 0\} \tag{2.28}$$

is a bijection.

2. *Let E_1 and E_2 be elliptic curves corresponding to the lattices Λ_1 and Λ_2. Then, the natural inclusion*

$$\{\textit{isogenies } \psi : E_1 \mapsto E_2\} \mapsto \{\textit{ maps } \psi : \mathbb{C}/\Lambda_1 \mapsto \mathbb{C}/\Lambda_2, \psi(0) = 0\} \tag{2.29}$$

is a bijection.

Let $E_1/\mathbb{C}$ and $E_2/\mathbb{C}$ be elliptic curves associated with the lattices Λ_1 and Λ_2, as described in 2.2.4. Then we consider that E_1 and E_2 are isomorphic over $\mathbb{C}$, if and only if Λ_1 and Λ_2 are homothetic. This means that there exists some $\alpha \in \mathbb{C}$ such that $\Lambda_1 = \alpha\Lambda_2$. Since the maps ψ_α are homomorphisms, it implies that every complex analytic map, from $E_1(\mathbb{C})$ to $E_2(\mathbb{C})$ which maps O to O, is necessarily a homomorphism. This is the analytic counterpart of which states that every isogeny of elliptic curves is a homomorphism. Therefore, we can now state what is shown below.

Theorem 2.2.5. *The following categories are equivalent:*

1. *Objects: elliptic curves,*
   Maps: isogenies.

2. *Objects: elliptic curves over $\mathbb{C}$,*
   Maps: complex analytic maps taking O to O.

3. *Objects: lattices $\Lambda \subset \mathbb{C}$ up to homotety,*
   Maps: $\phi(\Lambda_1, \Lambda_2) = \{\alpha \in \mathbb{C} : \alpha\Lambda_1 \subset \Lambda_2\}$.

cite

2.3 Alternative complex analytic uniformisation

We can not find a direct way to translate the uniformisation that we have done for elliptic curves over $\mathbb{C}$ above on the p-adic numbers, as they do not have any discrete lattices.
Therefore, we look for another way to express the uniformisation of elliptic curves on $\mathbb{C}$. We want to obtain a set of functions that could translate the conditions of 2.1.4 in a different environment. So, we consider the exponentiate map $\psi : z \mapsto e^{2\pi i z}$.
As said before in 2.1.3, we can normalise a lattice Λ with an homotety; this let us study the lattice $\Lambda_\tau = \mathbb{Z}\tau + \mathbb{Z}$ where $\tau \in \mathbb{C}, \Im\mathrm{m}(\tau) \geq 0$. The Weierstrass $\wp$-function related to Λ_τ satisfies:

$$\wp(z, \tau + 1) = \wp(z; \tau). \tag{2.30}$$

We can define of $u = e^{2\pi i z}$. We also consider $q = e^{2\pi i \tau}$ and find a Fourier expansion of $\wp$ in terms of u and q. Note that $|q| < 1$. This consideration induces an isomorphism:

$$\mathbb{C}/\Lambda \mapsto \mathbb{C}^*/q^{\mathbb{Z}}, \tag{2.31}$$

$$z \mapsto e^{2\pi i z}. \tag{2.32}$$

Our primary objective now is to derive an explicit formula for $\wp$ in this new way.

Remark 2.3.1. In order to find them, we need to derive new conditions that make it useful. In the previous chapter, the conditions on F, elliptic function related to a lattice Λ, were:

1. F is a meromorphic function on $\mathbb{C}$;
2. $F(z+\omega) = F(z), \qquad \forall z \in \mathbb{C}, \omega \in \Lambda$;
3. F is non constant and has a double poles at each point $\omega \in \Lambda$.

Therefore, we look for a meromorphic function $F(u;q)$ that meets the following criteria:

1. $F(q^k u;q) = F(u;q)$;
2. F has a double pole at each $u \in q^{\mathbb{Z}}$, and it is holomorphic outside of this.

The primary concept in developing such a function is to identify an appropriate function that meets condition 2 at $z = 1$, and then we make adjustments as needed to guarantee convergence. Now we consider the simplest function with a double pole at $X = 1$, that is, $F(X) = (1-X)^{-2}$, which makes us examine the following series:

$$\sum_{n\in\mathbb{Z}} \frac{1}{(1-q^n u)^2} \tag{2.33}$$

in the limit $n \mapsto \infty$ this sum doesn't converge as $|q| < 1$ as for

$$\lim_{n\mapsto\infty} q^n = 0 \implies \lim_{n\mapsto\infty} \left| \frac{1}{(1-q^n u)^2} \right| = 1. \tag{2.34}$$

Instead, we should consider $\frac{x}{(1-X)^2}$ to ensure convergence; as it is shown below.

Lemma 2.3.2.

1. *We define the function F as follows:*

$$F(u,q) = \sum_{n\in\mathbb{Z}} \frac{q^n u}{(1-q^n u)^2} \tag{2.35}$$

   converges absolutely and uniformly on compact subsets of $\mathbb{C}^*/q^{\mathbb{Z}}$.

2. *F is an elliptic function for a lattice Λ_τ and satisfies 1 and 2.*

3. *The Laurent series for F around $z = 0$ is of the form:*

$$F(u,q) = \frac{1}{(2\pi i)^2 z^2} - \left\{ \frac{1}{12} - 2\sum_{n\geq 1} \frac{q^n}{(1-q^n)^2} \right\} + \textit{(powers of } z\textit{)}. \tag{2.36}$$

The proof of the lemma is given in [7, Theorem I.6.1] .
We now relate this function back to $\wp$. By considering the start of the Laurent series of $\wp$ and subtracting the Laurent series of F. We consider the function:

$$\mu := \frac{1}{(2\pi i)^2}\wp(u;q) - F(u;q) + \frac{1}{12} - 2\sum_{n\in\mathbb{Z}} \frac{q^n}{(1-q^n)^2}. \tag{2.37}$$

We know that μ is holomorphic and elliptic, which implies that it is constant; moreover, it is thus identically zero, since it vanishes at 0. We also require a q-expansion for $\wp'$. We use

$$\frac{d}{dz} = 2\pi i u \frac{d}{du} \tag{2.38}$$

and obtain

$$\frac{1}{(2\pi i)^3}\wp'(u;q) = \sum_{n\in\mathbb{Z}} \frac{q^n u(1+q^n u)}{(1-q^n u)^3}. \tag{2.39}$$

Next, we perform a variable substitution to eliminate the powers of $(2\pi i)^3$ and the constant term $1/12$:

$$\frac{1}{(2\pi i)^2}x = x' + \frac{1}{12}, \tag{2.40}$$

$$\frac{1}{(2\pi i)^3}y = 2y' + x. \tag{2.41}$$

Under this substitution, the equation

$$y^2 = 4x^3 - g_2 x - g_3 \tag{2.42}$$

becomes

$$y^2 + xy = x^3 + B(q)x + C(q), \tag{2.43}$$

this for B, and C functions of q with

$$B(q) = -\frac{1}{4}\cdot\frac{1}{(2\pi i)^6}g_3(\tau) - \frac{1}{48}, \tag{2.44}$$

$$C(q) = -\frac{1}{4}\cdot\frac{1}{(2\pi i)^4}g_2(\tau) + \frac{1}{48}\cdot\frac{1}{(2\pi i)^4}g_2(\tau) + \frac{1}{1728}. \tag{2.45}$$

Theorem 2.3.3. *We define the series:*

$$X(u;q) = \sum_{n\in\mathbb{Z}} \frac{q^n u}{(1-q^n u)} 2 - 2\sum_{n\geq 1}\frac{q^n}{1-q^n}, \tag{2.46}$$

$$Y(u;q) = \sum_{n\in\mathbb{Z}} \frac{(q^n u)^2}{(1-q^n u)^3} + \sum_{n\geq 1}\frac{q^n}{1-q^n}. \tag{2.47}$$

Then, the map is an isomorphism.

$$\mathbb{C}^*/q^{\mathbb{Z}} \mapsto E_q : y^2 + xy = x^3 + B(q)x + \mathbb{C}(q), \tag{2.48}$$

$$u \mapsto \begin{cases} (X(u;q), Y(u;q)) : u \notin q^{\mathbb{Z}} \\ O : u \in q^{\mathbb{Z}} \end{cases} \tag{2.49}$$

cite

Chapter 3

Elliptic curves over p-adic fields

3.1 Local fields

Now we want to study elliptic curves over a different field which has more properties. Therefore, we shift our focus to non-archimedean local fields.
A local field is a field that is complete with respect to a nontrivial absolute value. The most common examples of local fields are real numbers $\mathbb{R}$ and complex numbers $\mathbb{C}$, equipped with their usual absolute values. For a more in-depth analysis, see [10, Chapter 1]. In order to study local fields, we should start by giving the definition of the absolute value.

Definition 3.1.1. An absolute value is a function $|\cdot| : K \mapsto R^+$ such that:

1. $|x| > 0$ if $x \neq 0$;
2. $|x \cdot y| = |x| \cdot |y|$;
3. $|x + y| \leq |x| + |y|$;
4. if $|x| < |y|$, then $|x \pm y| = |y|$.

The difference between archimedean and non-archimedean absolute values is:

1. A non archimedean absolute value satisfies
$$|x_1 + x_2 + \ldots x_n| \leq max|x_i| \textit{ (ultra metric inequality)}; \tag{3.1}$$
2. An archimedean absolute value does not satisfy the previous inequality.

We know that the only local fields that are not archimedean are equivalent to either a finite extension of $\mathbb{Q}_p$ or to $\mathbb{F}_q((T))$, for $\mathbb{F}_q$ a finite field.

Definition 3.1.2. A valuation v is a function:
$$v : K^* \mapsto R \tag{3.2}$$
such that $\forall x, y \in K^*$. It satisfies the properties:

1. $v(xy) = v(x) + v(y)$;

2. $v(x + y) \geq min v(x), v(y)$.

Given a valuation and a value $0 < \alpha < 1$, we can define the absolute value related to the valuation as follows:

$$|\cdot| = \alpha^{v(\cdot)}. \tag{3.3}$$

This defines a non archimedean absolute value.

Definition 3.1.3. Let K be a local field, then we can define some sets related to a valuation v or an alternative to an absolute value $|\cdot|$:

1. $\mathcal{O} := \{x \in K : v(x) \geq 0\} = \{x \in K : |x| \leq 1\}$. The set $\mathcal{O}$ is called the ring of integers of K with respect to the valuation v.

2. $\mathfrak{M} := \{x \in K : v(x) > 0\} = \{x \in K : |x| < 1\}$. The set $\mathfrak{M}$ is called the maximal ideal of the valuation v.

3. The set $R^* = \{x \in K : v(x) = 0\} = \{x \in K : |x| = 1\}$ is the set of invertible (units) elements of the ring $\mathcal{O}$.

4. The field $k = \mathcal{O}/\mathfrak{M}$ is called the residue field of the valuation v.

5. π an element in R such that $\mathfrak{M} = \pi\mathcal{O}$. π is called an uniformiser for R.

In the following pages, we set a normalised valuation as one in which $v(\pi) = 1$. These sets let us define a discrete valuation ring (DVR). This is an integral domain R with discrete valuation v. Specifically, it is a principal ideal domain that has precisely one nonzero maximal ideal $\mathfrak{M}$. In other words, a DVR R is a ring such that every element can be written uniquely (up to a unit) as a product of a power of a fixed prime element π. Now that we have described the general settings, we give a more precise description of the p-adic numbers as an extension of $\mathbb{Q}$ that arises from completing $\mathbb{Q}$ given the p-adic absolute value $|\cdot|_p$.
Since $v_p(x)$ is the p-adic valuation of x which is the largest integer n such that p^n divides x.
The p-adic valuation v_p has the following properties:

1. $v_p(xy) = v_p(x) + v_p(y)$;

2. $v_p(x + y) \geq min\{v_p(x), v_p(y)\}$.

That is why we define the p-adic absolute value for any $x \in \mathbb{Q}/\{0\}$ as $|x|_p = p^{-v_p(x)}$.
For example, $v_2(8) = 3$ since 2^3 divides 8 evenly, while $v_2(15) = 0$ since 2 does not divide 15. Therefore, $|8|_2 = 2^{-3} = \frac{1}{8}$ and $|15|_2 = 2^0 = 1$.
In $\mathbb{Q}_p$ we can write numbers differently as there exists a unique p-adic expansion in the form:

$$\sum_{n=-\infty}^{n=+\infty} a_n p^n, \qquad \text{where} a_n \in \mathbb{F}_p \text{finite field with } p \text{ elements.} \tag{3.4}$$

For instance for $p = 5$ we can write $\frac{1}{2} = \cdots 2223$. To find this expansion, we note that we can write rational numbers in the following way:

$$m/n = a + b\frac{1}{1-p^r} \text{ where } a \in \mathbb{Z}, r \in \mathbb{N} \text{ and } b \in \{0, \dots p^{r-1} - 1\}; \tag{3.5}$$

then we just need to note that $|p|_p < 1$. We use Cauchy sequences in $\mathbb{Q}$ with the $|\cdot|_p$ norm to complete $\mathbb{Q}$ by adding all points that are limits of Cauchy sequences with the p-adic norm.
We have some example that shows that $\mathbb{Q}_p$ are distinct from $\mathbb{R}$ as extensions of $\mathbb{Q}$. For example, $x^2 - p = 0$ has 2 solutions in $\mathbb{R}$, while it has no solution in $\mathbb{Q}_p$; conversely, $x^2 - 1 + p^3 = 0$ has a solution in $\mathbb{Q}_p$ while none in $\mathbb{R}$. Hence, there is no inclusion from one to the other.
We can also construct an example concretely.

Example 3.1.4. *Let $p = 5$ and we construct a $|\cdot|_5$-Cauchy sequence $(a_n) \in \mathbb{Q}$ such that*

1. $a_n^2 + 1 \equiv \pmod{5^n}$;
2. $a_{n+1} \equiv a_n \pmod{5^n}$.

We will construct it with induction. Base case: let $a_1 = 2$. Induction step: let a_n satisfy the previous conditions. Then, $\exists c \in \mathbb{Z}$ such that $a_n^2 + 1 = 5^n c$.
Therefore, for a_{n+1}, we must find a $b \in \mathbb{Z}$ that satisfies

$$a_{n+1}^2 + 1 = (a_n^2 + 5^n b)^2 + 1 \equiv 5^n(c + 2a_n b) \pmod{5^{n+1}}. \tag{3.6}$$

It is always possible to find such a b; since a_n is a $|\cdot|_p$ Cauchy sequence, the limit $X^2 + 1$ is in the completion of $\mathbb{Q}$, as it is not rational. We must be careful not to label it i, as we cannot differentiate between i and $-i$ in $\mathbb{Q}_p$.

We can now give the same sets that we defined before in the general settings but in $\mathbb{Q}_p$.

Definition 3.1.5. Let K be a field, we can then define some sets related to a valuation $v_p(\cdot)$ or alternative to an absolute value $|\cdot|_p$:

1. $\mathbb{Z}_p := \{x \in K : |x| \leq 1\}$. The set $\mathbb{Z}_p$ is called the set of p-adic integers.
2. $p\mathbb{Z}_p := \{x \in K : |x| < 1\}$. The set $p\mathbb{Z}_p$ is called the maximal ideal.
3. The set $\mathbb{Z}_p^* = \{x \in K : |x| = 1\}$ is the set of invertible (units) elements of the ring $\mathbb{Z}_p$.
4. The field $k = \mathbb{Z}_p/\mathfrak{M} \cong \mathbb{F}_p$ is called the residue field.
5. π an element in $\mathbb{Z}_p$ such that $p\mathbb{Z}_p = \pi\mathbb{Z}_p$. π is called an uniformiser for $\mathbb{Z}_p$.

3.2 Elliptic curves on local fields

In this section and in the following one, we study elliptic curves over non archimedean fields. As described before, let R be the ring of integers of K non-archimedean local field and let π be a uniformiser. Elliptic curves on the local field K have the same properties described in the first chapter. In addition, we can define the Weierstrass equation that minimises the value of $v(\Delta)$ as follows.

Definition 3.2.1. Let E/K be an elliptic curve. The minimal Weierstrass equation for the elliptic curve is the Weierstrass equation in the form

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \tag{3.7}$$

where all $a_1, a_2, a_3, a_4, a_6 \in R$. We can find by substituting $(x, y) \mapsto (u^{-2}x, u^{-3}y)$ Therefore, $v(\Delta) \geq 0$ we take the Weierstrass equation which minimises the value of $v(\Delta)$.

Theorem 3.2.2. *1. Every elliptic curve E/K has a minimal Weierstrass equation;*

2. *a minimal Weierstrass equation is unique up to a change of coordinates:*

$$x = u^2x' + r \qquad y = u^3y' + u^2sx' + t \tag{3.8}$$

with $u \in R^*, r, s, t \in R$.

3. *if we start with a Weierstrass equation with coefficients in R, then any change of coordinates that create a minimal equation:*

$$x = u^2x' + r \qquad y = u^3y' + u^2sx' + t \tag{3.9}$$

satisfies with $u \in R^*, r, s, t \in R$.

The proof is given in [8, theorem VII.3.2].
The equation is minimal if all the $a_i \in R$. Then we can change the coordinates with a new equation with $\Delta' = u^{-12}\Delta \in R$. Therefore,

$$a_i \in R \text{ and } v(\Delta) < 12 \Rightarrow \text{the equation is minimal.} \tag{3.10}$$

In the same way,

$$c_4' = u^{-4}c_4, c_6' = u_{-6}c_6 \tag{3.11}$$

$$a_i \in R \text{ and } v(c_4) < 4 \Rightarrow \text{the equation is minimal.} \tag{3.12}$$

$$a_i \in R \text{ and } v(c_6) < 6 \Rightarrow \text{the equation is minimal.} \tag{3.13}$$

For example, we can consider the elliptic curve $E/\mathbb{Q}_p$:

$$E : y^2 + xy + y = x^3 + x^2 + 22x - 9 \tag{3.14}$$

We can use the formulas in 1.1.3, to find $\Delta = -2^{15}5^2$ and $c_4 = -5 \cdot 211$, $c_6 = 2 \cdot 11 \cdot 13 \cdot 479$. As all the a_i are in $\mathbb{Z}_p$ for all p, and for all $p \geq 3$, $0 \leq v(\Delta) < 12$ imply that the Weierstrass equation is minimal. While, for $p = 2$ both $v_p(c_4) < 4$ and $v_p(c_6) < 6$ imply that the Weierstrass equation is minimal.

3.3 Reduction of elliptic curves

We define a function called reduction modulo π as the operation where k is the finite field which is the residue field R/π, which is the following:

$$\tilde{\phi} : R \mapsto k = R/\pi R \tag{3.15}$$

$$t \mapsto \tilde{t}. \tag{3.16}$$

So, given a minimal Weierstrass equation for E , we reduce the coefficients $a_i \in R$ to $\tilde{a_i} \in k$ to find

$$\tilde{E} = y^2 + \tilde{a_1}xy + \tilde{a_3}y = x^3 - \tilde{a_2}x^2 + \tilde{a_4}x + \tilde{a_6}. \tag{3.17}$$

$\tilde{E}$ is the reduction of E modulo π . We can do the same for each $P \in E(K)$.
We can define the following map:

$$E(K) \mapsto E(k) \tag{3.18}$$

$$P = [x_0, y_0, z_0] \mapsto \tilde{P} = [\tilde{x_0}, \tilde{y_0}, \tilde{z_0}] \tag{3.19}$$

The curve we obtain $\tilde{E}$ can be singular, but the non-singular points of the curve form a group $\tilde{E}_{ns}(k)$. Therefore, we are interested in studying the following subsets of $E(K)$ the elliptic curve over K.

$$E_0(K) = \{P \in E(K) : \tilde{P} \in \tilde{E}_{ns}(k)\} \tag{3.20}$$

$$E_1(K) = \{P \in E(K) : \tilde{P} = \tilde{O}\} \tag{3.21}$$

Remark 3.3.1. The set $E_0(K)$ is the set of points where the reduction map gives non singular points, while $E_1(K)$ is the kernel of the reduction map. Those two sets do not change on the basis of the minimal Weierstrass equation.

Definition 3.3.2. Let E be an elliptic curve over a local field K, and we study $\tilde{E}$ obtained with the reduction modulo π as we have seen the different cases in 1.1.4-1 :

1. E has good (or stable) reduction if $\tilde{E}$ is non singular;
2. E has multiplicative (or semistable) reduction if $\tilde{E}$ has a node;
3. E has additive (or unstable) reduction if $\tilde{E}$ has a cusp.

Remark 3.3.3. In cases 2,3 it is said to have a bad reduction.
In case 2, E has multiplicative reduction, therefore, $\exists! P \in E$ so that it is singular. At this point, if the tangents have coefficients in k then we say that E has **split** multiplicative reduction; otherwise, we call it **non-split**.

Theorem 3.3.4. *Let E/K be an elliptic curve given by a minimal Weierstrass equation:*

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6. \tag{3.22}$$

Let Δ be the discriminant of this equation and let c_4 be the usual expression involving $a_1, ..., a_6$ as described in 1.1.1.

1. *E has good reduction if and only if* $v(\Delta) = 0$*; which is equivalent to condition* $\Delta \in R^*$*. In this case* $\tilde{E}/k$ *is an elliptic curve.*

2. *E has multiplicative reduction if and only if* $v(\Delta) > 0$ *and* $v(c_4) = 0$*; with equivalent condition as* $\Delta \in \mathfrak{M}$ *and* $c_4 \in R$*. In this case* $\tilde{E}_{ns}$ *is the multiplicative group,*$\tilde{E}_{ns}(\overline{k}) \cong \overline{k}^*$.

3. *E has additive reduction if and only if* $v(\Delta) > 0$ *and* $v(c_4) > 0$*; if for example* $\Delta, c_4 \in M$*. In this case* $\tilde{E}_{ns}$ *is the additive group,* $\tilde{E}_{ns}(\overline{k}) \cong \overline{k}^+$.

Proof. To prove this theorem we have the reduction types applying the previous definition to 1.1.4 and then we apply theorem 1.2.3. □

We now study the cases of the reduced Weierstrass equation over k.

Example 3.3.5. *Let* $p \geq 5$ *be a prime. Then the elliptic curve*

$$E_1 : y^2 = x^3 + px^2 + 1 \tag{3.23}$$

has good reduction over $\mathbb{Q}_p$ *as*

$$\tilde{E_1} : y^2 = x^3 + 1 \tag{3.24}$$

is an elliptic curve; while

$$E_2 : y^2 = x^3 + x^2 + p \tag{3.25}$$

has (split) multiplicative reduction over $\mathbb{Q}_p$ *as*

$$\tilde{E_2} : y^2 = x^3 + x^2 \tag{3.26}$$

has a singular point in $(0, 0)$ *and it is a node and*

$$E_3 : y^2 = x^3 + p \tag{3.27}$$

E_3 *has additive reduction over* $\mathbb{Q}_p$ *by a similar analysis.*

Remark 3.3.6. Moving to the extension field $Q(\sqrt{6})_p$, E_3 achieves good reduction, as a substitution

$$x \to \sqrt[3]{p}x, \qquad y \to \sqrt{p}y \tag{3.28}$$

results in a minimal Weierstrass equation with good reduction as follows:

$$py^2 = px^3 + p \implies y^2 = x^3 + 1. \tag{3.29}$$

In contrast, curve E_2 exhibits multiplicative reduction over any extension of $\mathbb{Q}_p$. Typically, by extending the base field, additive reduction is converted into either multiplicative or good reduction. This explain the meaning of the terms stable, semistable, and unstable. When an elliptic curve E/K has bad reduction, it is advantageous to find if it can obtain good reduction over an extension of K, which can be done as shown in 3.3.8.

We now want to study when is it possible to find an extension that can simplify our analysis.

Definition 3.3.7. Let E/K be an elliptic curve. We say that E/K has potential good reduction if there exists a finite extension K'/K such that E has good reduction over K'.

Theorem 3.3.8. *(Semistable reduction theorem) Let E/K be an elliptic curve.*

1. *Let K'/K be a finite extension. If E has both good and multiplicative reduction over K, it retains the same reduction type over K'.*
2. *There exists a finite extension K'/K such that E has either good or (split) multiplicative reduction over K'.*

The proof is given in [8, Theorem VII.5.4] with the condition that $char(K) > 5$ while for a complete proof see [7, Chapter IV.9] which is a complete proof but it utilise the Neron Model of an elliptic curve.

Lemma 3.3.9. *Let E/K be an elliptic curve. Then E has potential good reduction if and only if its j-invariant is integral, for example, if and only if $j(E) \in R$.*

The proof is found in [8, Theorem VII.5.5] and [8, A.1.4b]. Recall that the subgroup $E_0(K)$ consists of the elements of $E(K)$ that do not map to a singular point of $E(k)$. We can now consider the quotient $E(K)/E_0(K)$. The most crucial aspect of this quotient is its finiteness.

Theorem 3.3.10. *(Kodaira, Néron) Let E/K be an elliptic curve. If E has split multiplicative reduction over K, then $E(K)/E_0(K)$ is a cyclic group of order $v(\Delta) = -v(j)$. In all other cases, the group $E(K)/E_0(K)$ is finite and has order at most 4.*

The proof is complex and uses the Neron model, it is proven in [7, Chapter IV.8]

Lemma 3.3.11. *The subgroup $E_0(K)$ has finite index in $E(K)$.*

[8, Lemma VII.6.2]

Chapter 4

Tate curves and p-adic uniformisation

4.1 Tate curves

As seen before, the elliptic curves on $\mathbb{C}$ have a parametrisation over $\mathbb{C}/\Lambda$ 2.2.2. We want to replace $\mathbb{C}$ with $\mathbb{Q}_p$. However, we cannot immediately translate this approach. In fact, $\mathbb{Q}_p$ only has the trivial lattice. Suppose that $\Lambda \subset \mathbb{Q}_p$ is a subgroup and $t \in \Lambda$, then

$$p^n t \in \Lambda \text{ and } lim_{n\to\infty} p^n t = 0. \tag{4.1}$$

So, 0 is an accumulation point for all Λ, therefore there isn't any non-trivial lattice.
As we have seen in the alternative case of complex uniformisation 2.3.3, we can try a different approach by using the exponentiation map to obtain an isomorphism between $\mathbb{C}^*$ and elliptic curves over $\mathbb{C}$.
We can consider $\mathbb{Q}_p^*$, which has discrete subgroups that we can construct as follows: given $q \in \mathbb{Q}_p^*$ and $|q| < 1$. So, we construct $q^{\mathbb{Z}} = \{q^n : n \in \mathbb{Z}\}$, which is a discrete subgroup.
Starting from discrete subgroups of $\mathbb{Q}_p$, we can try to mimic the complex case in order to find an isomorphism between $\mathbb{Q}^*/q^{\mathbb{Z}}$ and elliptic curves over $\mathbb{Q}_p$. In the following section, we consider finite extensions K of $\mathbb{Q}_p$.

Lemma 4.1.1. *Let $(K, |\cdot|_p)$ be a field with p-adic absolute value and $q \in K$ with $|q|_p < 1$. We define the series :*

$$s_k(q) = \sum_{n\geq 1} \frac{n^k q^n}{1-q^n} = \sum_{n\geq 1} \sigma_k(n) q^n, \tag{4.2}$$

which converges on $\mathbb{Z}_p$, where $\sigma_k(n) = \sum_{d|n} d^k$. Thus, let us define the following series on $\mathbb{Z}_q$:

$$a_4(q) = -5s_3(q), \tag{4.3}$$

$$a_6(q) = -\frac{5s_3(q) + 7s_5(q)}{12}. \tag{4.4}$$

The series $a_4(q)$ and $a_6(q)$ converge in K for all $q \in K$ if $|q|_p < 1$.

Proof. The proof of the convergence of the series $s_k(q)$ follows immediately from the following facts. Let K be a p-adic field with norm $|\cdot|_p$ and we denote $v_p(\cdot)$ as the valuation related to the absolute value $|\cdot|_p$.
A series $\sum_{n\geq 1} a_n$ with $a_n \in K$ is convergent if and only if $|a_n| \mapsto 0$ whenever $n \mapsto \infty$. $s_k(q)$ converges as the elements of the sum of $s_k(q)$ converge as follows:

$$v_p(\frac{n^k q^n}{1-q^n}) \leq k v_p(n) + n v_p(q) + min[v_p(1), n v_p(q)]. \tag{4.5}$$

Then, as $v(q)_p > 1$, we have the convergence of $s_k(q)$.
We substitute the formula of $s_3(q)$ into $a_4(q)$ to find:

$$a_4(q) = -5 s_3(q) = -5 \sum_{n\geq 1} \frac{n^3 q^n}{1-q^n}. \tag{4.6}$$

Then,

$$v_p(n^3 \frac{q^n}{1-q^n}) = v_p(n^3) + v_p(\frac{q^n}{1-q^n}) = 3v_p(n) + n v_p(q) - v_p(1-q^n). \tag{4.7}$$

We now know that

$$v_p(1-q^n) \leq inf\{v_p(1), v_p(-q^n)\}, \tag{4.8}$$

where $v_p(1) = 0$ and, as $|q| < 1$, $v_p(q) > 1$. Hence,

$$v_p(1-q^n) = inf\{v_p(1), v_p(-q^n)\} = 0. \tag{4.9}$$

Therefore, we get:

$$v_p(n^3 \frac{q^n}{1-q^n}) = 3v_p(n) + n v_p(q) - v_p(1-q^n) = 3v_p(n) + n v_p(q). \tag{4.10}$$

If we let n tend to infinity, we can see that $v_p\left(n^3 \frac{q^n}{1-q^n}\right)$ also tends to infinity, which proves that the series $a_4(q)$ is convergent.
In order to demonstrate that the series $a_6(q)$ is convergent, first we will show that the coefficients of $a_6(q)$ are in $\mathbb{Z}$. Consider $a_6(q)$ as a power series in q

$$a_6(q) = -\frac{5s_3(q) + 7s_5(q)}{12} = -\frac{5\sum_{n\geq 1} \sigma_3(q) q^n + 7\sum_{n\geq 1} \sigma_5(q) q^n}{12} \tag{4.11}$$

$$= -\frac{\sum_{n\geq 1} [5\sigma_3(q) + 7\sigma_5(q)]}{12}. \tag{4.12}$$

We now want to prove that:

$$5\sigma_3(q) + 7\sigma_5(q) \equiv 0 \pmod{12}. \tag{4.13}$$

We see that

$$5\sigma_3(q) + 7\sigma_5(q) = 5\sum_{d|q} d^3 + 7\sum_{d|q} d^5 = \sum_{d|q}\left[5d^3 + 7d^5\right]. \tag{4.14}$$

Therefore, to prove 4.13, it is enough to demonstrate that

$$5d^3 + 7d^5 \equiv 0 \pmod{12}, \tag{4.15}$$

where $d \in Z$. After studying some cases, it can be easily seen that it is true. □

Definition 4.1.2. The Tate curve E_q is defined by the equation

$$E_q := y^2 + xy = x^3 + a_4(q)x + a_6(q). \tag{4.16}$$

We can study the Tate curve to find its properties.

Theorem 4.1.3. *The Tate curve E_q is an elliptic curve with the discriminant*

$$\Lambda(E_q) = q\prod_{n\geq 1}(1-q^n)^{24}, \tag{4.17}$$

and j-invariant

$$j(E_q) = \frac{1}{q} + 1 + 744 + 196884q + \dots = \frac{1}{q} + \sum_{n\geq 0} c(n)q^n \tag{4.18}$$

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

Proof. The discriminant of E_q is given by a formula that we have in 1.1.3 which refers to elliptic curve. The discriminant is then written with the q-expansions of $a_4(q)$ and $a_6(q)$ as follows:

$$\Delta(q) = q - 24q^2 + 252q^3 + \cdots \equiv q \pmod{q^2}. \tag{4.19}$$

Hence, $|\Delta(q)| = |q|$ and $|q| \neq 0$ on K^*, so E_q has no singular point and E_q is an elliptic curve. The Jacobi product formula for the determinant $\Delta(E_q) = q\prod_{n\geq 1}(1-q^n)^24$ is applicable for all $q \in \mathbb{C}$, is valid as a formal power series in $\mathbb{Z}[q]$, when we take q with $|q|_p < 1$.
Finally, we derive the formula:

$$j(q) = \frac{(1+48a_4(q))^3}{\Delta(q)}, \tag{4.20}$$

which we can write also as

$$j(q) = \frac{1}{q}(1 + 744q + 196884q^2 + \dots). \tag{4.21}$$

We calculated it directly by taking the quotient of the appropriate power series formally and we find that the discriminant and the j-invariant are well defined for E_q. □

Remark 4.1.4. The coefficients of the Fourier of j and Δ are related to the Ramanujan τ-function. They have been studied for more than a century; for an analysis of progress in their calculation, see [1].

4.2 p-adic uniformization of Tate curves

Theorem 4.2.1. *Let $E_q \subset \mathbb{Q}_p$ and $q \in \mathbb{Q}_p^*$ with $|q| < 1$. The series*

$$X(u,q) = \sum_{n\in\mathbb{Z}} \frac{q^n u}{(1-q^n u)^2} - 2s_1(q) \tag{4.22}$$

$$Y(u,q) = \sum_{n\in\mathbb{Z}} \frac{(q^n u)^2}{(1-q^n u)^3} + s_1(q) \tag{4.23}$$

converge for all $u \in K$, $u \notin q^{\mathbb{Z}}$.

Proof. We now prove 4.2.1. We need to show that $s_1(q)$ is equal to $\sum_{n\geq 1} \frac{q^n}{(1-q^n)^2}$. Therefore, to understand this equality, we first observe that

$$\frac{T}{(1-T)^2} = T\frac{d}{dT}\left(\frac{1}{1-T}\right) = T\frac{d}{dT}\sum_{m\geq 0} T^m = \sum_{m\geq 1} mT^m. \tag{4.24}$$

This is possible as $|q^n| < 1$. Next, we replace $T = q^n$ and sum over $n \geq 1$, and we get

$$\sum_{n\geq 1} \frac{q^n}{(1-q^n)^2} = \sum_{n\geq 1}\sum_{m\geq 1} mq^{nm} = \sum_{m\geq 1} m\sum_{n\geq 1} q^{nm} = \sum_{m\geq 1} \frac{mq^m}{1-q^m}. \tag{4.25}$$

This, let us use the alternative way of writing $s_1(q) = \sum_{n\geq 1} \frac{q^n}{(1-q^n)^2}$. Therefore, we can rewrite 4.22 as

$$X(u,q) = \sum_{n\in\mathbb{Z}} \frac{q^n u}{(1-q^n u)^2} - 2\sum_{n\geq 1} \frac{q^n}{(1-q^n)^2}. \tag{4.26}$$

Let us consider the first sum in the series above:

$$\sum_{n\in\mathbb{Z}} \frac{q^n u}{(1-q^n u)^2} = \sum_{n\leq -1} \frac{q^n u}{(1-q^n u)^2} + \frac{u}{(1-u)^2} + \sum_{n\geq 1} \frac{q^n u}{(1-q^n u)^2} \tag{4.27}$$

where $\frac{u}{(1-u)^2}$ is the value of the series for $n = 0$. Then, we can rewrite $X(u,q)$ as

$$X(u,q) = \frac{u}{(1-u)^2} + \sum_{n\leq -1} \frac{q^n u}{(1-q^n u)^2} + \sum_{n\geq 1}\left[\frac{q^n u}{(1-q^n u)^2} - 2\frac{q^n}{(1-q^n)^2}\right]. \tag{4.28}$$

We want to subdivide again to find more insight. We consider

$$\sum_{n\leq -1} \frac{q^n u}{(1-q^n u)^2}; \tag{4.29}$$

then we change the sign of the index and we write it as

$$\sum_{n\geq 1} \frac{q^{-n} u}{(1-q^{-n} u)^2}, \tag{4.30}$$

and $X(u,q)$ becomes

$$X(u,q) = \frac{u}{(1-u)^2} + \sum_{n\geq 1}\left[\frac{q^n u}{(1-q^n u)^2} + \frac{q^{-n}u}{(1-q^{-n}u)^2} - 2\frac{q^n}{(1-q^n)^2}\right]. \tag{4.31}$$

Therefore, we multiply the numerator and the denominator of the third term of the series by $\frac{q^{2n}}{u^2}$ as follows:

$$\frac{q^{-n}u}{(1-q^{-n}u)^2}\cdot\frac{\frac{q^{2n}}{u^2}}{\frac{q^{2n}}{u^2}} = \frac{q^n u^{-1}}{(1-q^n u^{-1})^2}. \tag{4.32}$$

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

$$\frac{1}{u+u^{-1}-2} + \sum_{n\geq 1}\left[\frac{q^n u}{(1-q^n u)^2} + \frac{q^n u^{-1}}{(1-q^n u^{-1})^2} - 2\frac{q^n}{(1-q^n)^2}\right]. \tag{4.33}$$

Now, the objective is to see that this series is convergent we will use the fact that a series $\sum_{n=0}^{\infty} a_n x^n$ is convergent if and only if $v_p(a_n) \mapsto \infty$ as $n \mapsto \infty$. Now, by the properties of valuations

$$v_p\left(\frac{q^n u}{(1-q^n)^2} + \frac{q^n u^{-1}}{(1-q^n u^{-1})^2} - 2\frac{q^n}{(1-q^n)^2}\right) \tag{4.34}$$

$$\geq min\left\{v_p\left(\frac{q^n u}{(1-q^n u)^2}\right), v_p\left(\frac{q^n u^{-1}}{(1-q^n u^{-1})^2}\right), v_p\left(-2\frac{q^n}{(1-q^n)^2}\right)\right\}. \tag{4.35}$$

Let us consider the valuations separately. The first is the following:

$$v_p\left(\frac{q^n u}{(1-q^n u)^2}\right) = v_p(q^n) + v_p(u) - 2v_p(1-q^n u). \tag{4.36}$$

Here, since $v_p(1) \neq v_p(q^n u)$, we have $v_p(1-q^n u) = min\{v_p(1), v_p(q^n u)\} = v_p(1) = 0$. Hence, the first term becomes

$$v_p\left(\frac{q^n u}{(1-q^n u)^2}\right) = v_p(q^n) + v_p(u) = nv_p(q) + v_p(u). \tag{4.37}$$

The second valuation is

$$v_p\left(\frac{q^n u^{-1}}{(1-q^n u^{-1})^2}\right) = nv_p(q) - v_p(u) - 2v_p(1-q^n u^{-1}). \tag{4.38}$$

By a similar argument as above, we obtain $v_p(1-q^n u^{-1}) = 0$. Therefore it becomes

$$v_p\left(\frac{q^n u^{-1}}{(1-q^n u^{-1})^2}\right) = nv_p(q) - v_p(u) \tag{4.39}$$

Similarly, the third is

$$v_p\left(\frac{q^n}{(1-q^n)^2}\right) = v_p(q^n) - 2v_p(1-q^n)^2. \tag{4.40}$$

Here, $v_p(1-q^n)$ is equal to 0 by the same argument. So,

$$v_p\left(\frac{q^n}{(1-q^n)^2}\right) = v_p(q^n) = nv_p(q) \tag{4.41}$$

therefore,

$$v_p\left(\frac{q^n u}{(1-q^n)^2} + \frac{q^n u^{-1}}{(1-q^n u^{-1})^2} - 2\frac{q^n}{(1-q^n)^2}\right) \tag{4.42}$$

$$\geq min\{nv_p(q) + v_p(u), nv_p(q) - v_p(u), nv_p(q)\}. \tag{4.43}$$

which tends to infinity as $n \mapsto \infty$. Therefore, the series $X(u,q)$ is convergent.
Now, let us consider the series:

$$Y(u,q) = \sum_{n\in\mathbb{Z}} \frac{(q^n u)^2}{(1-q^n u)^3}. \tag{4.44}$$

Similarly to above, we can write it as

$$Y(u,q) = \frac{u^2}{(1-u)^3} + \sum_{n\geq 1}\left[\frac{(q^n u)^2}{(1-q^n u)^3} + \frac{q^n}{(1-q^n)^2}\right] + \sum_{n\leq -1}\frac{(q^n u)^2}{(1-q^n u)^3}. \tag{4.45}$$

Now, we can write the third term in the sum as

$$\sum_{n\geq 1}\frac{(q^{-n}u)^2}{(1-q^{-n}u)^3} \tag{4.46}$$

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

$$\sum_{n\geq 1}\frac{(q^{-n}u)^2}{(1-q^{-n}u)^3} \tag{4.47}$$

$$\sum_{n\geq 1}\frac{-q^n u^{-1}}{(1-q^n u^{-1})^3}. \tag{4.48}$$

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

$$Y(u,q) = \frac{u^2}{(1-u)^3} + \sum_{n\geq 1}\left[\frac{(q^n u)^2}{(1-q^n u)^3} - \frac{q^n u^{-1}}{(1-q^n u^{-1})^3} + \frac{q^n}{(1-q^n)^2}\right]. \tag{4.49}$$

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

$$v_p\left(\frac{q^n u)^2}{(1-q^n u)^3} - \frac{q^n u^{-1}}{(1-q^n u^{-1})^3} + \frac{q^n}{(1-q^n)^2}\right) \mapsto \infty \tag{4.50}$$

as $n \mapsto \infty$. Hence, $Y(u,q)$ is convergent. We can rewrite $X(u,q), Y(u,q)$ as follows:

$$X(u,q) = \frac{1}{u+u^{-1}-2} + \sum_{n\geq 1}\left(\frac{q^n u}{(1-q^n u)^2} + \frac{q^n u^{-1}}{(1-q^n u^{-1})^2} - 2\frac{q^n}{(1-q^n)^2}\right) \tag{4.51}$$

$$Y(u,q) = \frac{u^2}{(1-u)^3} + \sum_{n\geq 1}\left(\frac{(q^n u)^2}{(1-q^n u)^3} - \frac{q^n u^{-1}}{(1-q^n u^{-1})^3} + \frac{q^n}{(1-q^n)^2}\right). \tag{4.52}$$

These expressions show that $X(u,q)$ and $Y(u,q)$ converge for all $u \in \overline{K}^* \setminus q^{\mathbb{Z}}$. □

As we have proven before these properties of the series $X(u,q), Y(u,q)$ we can now prove the following theorem.

Theorem 4.2.2. *The series X, Y define a surjective homomorphism*

$$\phi : \overline{K}^* \longmapsto E_q(\overline{K}^*) \tag{4.53}$$

$$\phi = \begin{cases} (X(u,q), Y(u,q)) & \text{if } u \notin q^{\mathbb{Z}} \\ \mathbb{O} & \text{if } u \in q^{\mathbb{Z}}. \end{cases} \tag{4.54}$$

The kernel of the homomorphism ϕ is $q^{\mathbb{Z}}$.

Proof. Now we prove 4.2.2. We want to show that the image of the map ϕ is a subset of the Tate curve E_q given by the Weierstrass equation as follows:

$$E_q : = \ y^2 + xy = x^3 + a_4(q)x + a_6(q). \tag{4.55}$$

We find the following functional equations that help us to find a new formula for both X, Y with coefficients in $\mathbb{Q}(u)$:

$$X(qu,q) = X(u,q) = X(u^{-1},q) \tag{4.56}$$

$$Y(qu,q) = Y(u,q) \text{ and} \tag{4.57}$$

$$Y(u^{-1},q) = -Y(u,q) - X(u,q). \tag{4.58}$$

If we consider u just in the range $|q| < |u| < |q|^{-1}$, we obtain $|q^n u| < 1$ and $|q^n u^{-1}| < 1$ for $n \in \mathbb{N}$. Now, we are able to find a formula to rewrite X, Y with power series with coefficients in $\mathbb{Q}(u)$.
This help us to show that when we substitute the series $X(u,q)$ and $Y(u,q)$ for x and y in this equation, we get an identity valid for all $u \in \overline{K}^* \setminus q^{\mathbb{Z}}$. It is enough to consider values of u such that $|q| < |u| \leq 1$ and $u \neq 1$ based on the periodicity of X and Y. In this range, we can use the above formulas that express X and Y as power series in q with coefficients that are rational functions of u. Thus, we will be done if we can show that the equation

$$Y(u,q)^2 + X(u,q)Y(u,q) = X(u,q)^3 + a_4(q)X(u,q) + a_6(q) \tag{4.59}$$

is valid as an identity in the ring of formal power series in q with coefficients that are rational functions of the indeterminate u. In other words, we want to verify that this

identity holds in the ring $\mathbb{Q}(u)[q]$. Then, since u assumes different values, we deduce that the coefficients are formally equal as rational functions of u. Hence, we have an equality of formal power series in $\mathbb{Q}(u)[q]$.

We now want to prove that ϕ is a homomorphism.
We have to demonstrate that the map ϕ satisfies $\phi(u_3) = \phi(u_1) + \phi(u_2)$ where $u_1, u_2, u_3 \in \overline{K}^*$ and $u_3 = u_1 u_2$. In order to simplify the writing, we define $P_i := \phi(u_i)$. Then, since $\phi(qu) = \phi(u)$, ϕ is periodic. Without loss of generality, we can study only the case in which u_1 and u_2 are in the range $|q| < |u_1| \leq |1|$ and $|1| \leq |u_2| < |q|^{-1}$. This lets us have the following condition for u_3: $|q| < |u_3| < |q|^{-1}$. Therefore, they are all in the range of convergence of the power series expressions for $X, Y \in \mathbb{Q}(u)[q]$ as described above. Let us begin by examining the case where $u_1 = 1$ or $u_2 = 1$. For example, if we assume $u_2 = 1 \Rightarrow u_3 = u_1 * 1$, then according to the definition of ϕ, we have $\phi(u_3) = O + \phi(u_1)$.
Then, we study the cases $u_1 u_2 = 1$ and $\phi(u_3) = O$. Therefore, by $u_2 = u_1^{-1}$ and the functional equations $X(u, q) = X(u^{-1}, q)$ and $Y(u^{-1}, q) = -Y(u, q) - X(u, q)$. We obtain the following functional equations:

$$X(u_2, q) = X(u_1, q), \tag{4.60}$$

$$Y(u_2, q) = -Y(u_1, q) - X(u_1, q). \tag{4.61}$$

So $\phi(u_1) + \phi(u_2) = O$, therefore we have $\phi(u_3) = \phi(u_1) + \phi(u_2)$ formally. We also prove that $P_1 + P_2 = O \iff x_1 = x_2$ and $y_2 = -y_1 - x_1$ using the 1.2.2 for elliptic curves, as the Tate curve is an elliptic curve.

We now consider the remaining cases in which all $P_i \neq O$.
To simplify the formulas, we write $x_i := X(u_i, q)$ and $y_i := Y(u_i, q)$. The simpler case is where $x_1 \neq x_2$, because we find the following by 1.2.2 as before. We define λ and υ as $\lambda = \frac{y_2 - y_1}{x_2 - x_1}$ and $\upsilon = \frac{y_1 x_2 - y_2 x_1}{x_2 - x_1}$,, which let us find the following equations for x_3, y_3:

$$x_3 = \lambda^2 + a_1 \lambda - a_2 - x_1 - x_2, \tag{4.62}$$

$$y_3 = -(\lambda + a_1) x_3 - \upsilon - a_3. \tag{4.63}$$

Here, a_1, a_2, a_3 are defined in the Weierstrass equation of the Tate curve 1.1.3. We then find the following 2 equations:

$$x_3(x_2 - x_1)^2 = (y_2 - y_1)^2 + (y_2 - y_1)(x_2 - x_1) - (x_1 + x_2)(x_2 - x_1)^2, \tag{4.64}$$

$$y_3(x_2 - x_1) = x_3(y_1 - y_2 + x_1 - x_2) - (y_1 x_2 - y_2 x_1). \tag{4.65}$$

All these identities hold for all u_1, u_2, q as defined in the ranges. Therefore, these are true identities in the formal powers $\mathbb{Q}(u_1, u_2)[[q]]$, the ring of the formal power with coefficients in $\mathbb{Q}(u_1, u_2)$. So, this is true in the field K in which we work.

To prove the final case $x_1 = x_2$, we consider the useful fact explained below.

Lemma 4.2.3. *If $\psi : K^* \longmapsto E_q(K)$ takes infinitely many distinct values and satisfies*

$$\psi(u_1 u_2) = \psi(u_1) + \psi(u_2) \text{ if } \psi(u_1) \neq \pm\psi(u_2). \tag{4.66}$$

Then ψ is a homomorphism.

In order to prove that

$$\phi : K^* \longmapsto E_q(K) \tag{4.67}$$

is a homomorphism, we only need to show that ϕ takes infinite values. For example, the series for $X(u,q)$ has that for any $t \in K$ with $|t| < 1$, we have $|X(1+t,q)| = |t|^{-2}$. Thus, there are infinitely many values that are applicable. Therefore, we conclude that ψ is a homomorphism from K^* into $E_q(K)$. The fact that the kernel of ϕ is $q^{\mathbb{Z}}$ is clear from its definition. □

Theorem 4.2.4. *The map ϕ is surjective.*

Proof. We just need to show that the map ϕ is surjective. A more general proof given with p-adic analytics methods is given in [6, Chapter 3] We need to show that, for all $P \in E_q(K)$, it exists $u \in \overline{K}^*$ such that $\phi(u) = P$. We want to prove that for all L, finite extensions of K, the map $\phi : L^* \mapsto E_q(L)$ is surjective; this would imply the result we need.
We define the subsets of $E_q(K)$ where $\tilde{E}_q$ is the reduction of E_q modulo $\mathbb{Z}_p$, which is the maximal ideal of $\mathbb{Q}_p$. $\tilde{E}_q$ has the equation $y^2 + xy = x^3$.

$$E_{q,0}(K) = \{p \in E_q(K) : \tilde{P} \in \tilde{E}_{q,ns}(k)\} \tag{4.68}$$

$$E_{q,1}(K) = \{P \in E_q(K) : \tilde{P} = \tilde{O}\}, \tag{4.69}$$

where $\tilde{E}_{q,ns}$ are the non singular points on $\tilde{E}_q$. These let us define the filtration:

$$E_q(K) \supset E_{q,0}(K) \supset E_{q,1}(K), \tag{4.70}$$

and also the isomorphisims

$$E_{q,0}(K)/E_{q,1} \cong \tilde{E}_{q,ns} \text{ and } E_{q,1} \cong \widehat{E}_q(\mathfrak{M}) \tag{4.71}$$

$$P \mapsto \tilde{P}P = (x,y) \mapsto -\frac{x}{y}. \tag{4.72}$$

From [8, theorem VII.2.1]], [8, theorem VII.2.2] we have isomorphisms where $\widehat{E}$ is the formal group of E. In the same way $K^*/q^{\mathbb{Z}}$ admits the following filtration. This let us define

$$R_1^* = \{u \in R : u \equiv 1 \pmod{\mathfrak{M}}\} \tag{4.73}$$

as the group of units in R.

$$K^*/q^{\mathbb{Z}} \supset R^* \supset R_1^*, \tag{4.74}$$

which gives us another isomorphism

$$R^*/R_1^* \cong k^* \text{ and } R_1^* = \widehat{G}_m(\mathfrak{M}) \tag{4.75}$$

$$a \longmapsto \tilde{a} \text{ and } u \longmapsto 1 - u, \tag{4.76}$$

where $\widehat{G}_m$ is the formal multiplicative group 1.3.1
Now, we aim to prove that ϕ is an isomorphism and respects the filtrations described above. So, we start the proof with showing that $\phi(R_1^*) = E_{q,1}(K)$; we show both inclusions of sets,

we begin with $\phi(R_1^*) \subset E_{q,1}(K)$.
As $X(u,q)$ has formula

$$X(u,q) = \frac{u}{u^2+1-2u} + \sum_{n\geq 1}\left(\frac{q^n u}{(1-q^n u)^2} + \frac{q^n u^{-1}}{(1-q^n u^{-1})^2} - 2\frac{q^n}{(1-q^n)^2}\right), \tag{4.77}$$

it is true that

$$\text{if } u \cong 1 \pmod{\mathfrak{M}} \implies ord_v(X(u,q)) < 0. \tag{4.78}$$

We can say so, since $u/(u-1)^2$ is non-integral, this implies that $\phi(R_1^*) \subset E_{q,1}(K)$.
Now, let us prove the other inclusion $\phi(R_1^*) \supset E_{q,1}(K)$. We have the following map:

$$G_m(\mathfrak{M}) \xrightarrow{\cong} R_1^* \xrightarrow{\phi} E_{q,1}(K) \xrightarrow{\cong} \widehat{E}_q(\mathfrak{M}) \tag{4.79}$$

$$t \longmapsto \frac{X(1+t,q)}{Y(1+t,q)}. \tag{4.80}$$

We substitute $u = 1+t$ into the series for $X(u,q)$ and $Y(u,q)$ and expand as Laurent series in t. We find that

$$X(1+t,q) = t^{-2}\left(1 + \sum_{m\geq 1}\alpha_m t^m\right) \text{ and } Y(1+t,q) = t^{-3}\left(1 + \sum_{m\geq 1}\beta_m t^m\right), \tag{4.81}$$

where $\alpha_m, \beta_m \in R$. Then, since both $G_m(\mathfrak{M}), \widehat{E}_q(\mathfrak{M})$ are the same set $\mathfrak{M}$ with different operations attached, therefore, we want to show that the map

$$\psi : \mathfrak{M} \longmapsto \mathfrak{M} \tag{4.82}$$

$$t \longmapsto t\left(1 + \sum_{m\geq 1}\gamma_m t^m\right) \tag{4.83}$$

is surjective. We prove this by stating a simple result concerning power series.

Lemma 4.2.5. *Let $a \in R^*$ and $f(T) \in R[[T]]$ be a power series of the form*

$$f(T) = at + \textit{(higher order terms)}, \tag{4.84}$$

then there is a unique power series $g(T) \in R[[T]]$ that satisfy $f(g(T)) = T$ and $g(T)$ satisfy also $g(f(T)) = T$.

The proof is given by induction, and then it shows that if another power series exists, it is the same as the one previously found. The complete proof is given in [8, Chapter IV.2] .
This is helpful as we can now apply this lemma to ψ, so let us find a power series $\lambda(w) \in \mathfrak{M}$ such that $\psi(\lambda(w)) = w$. This proves the inclusion $\phi(R_1^*) \supset E_{q,1}(K)$, which then implies $\phi(R_1^*) = E_{q,1}(K)$.
We can now study ϕ on R^* to prove that $\phi(R^*) = E_{q,0}(K)$.
As before, we prove the inclusion $\phi(R^*) \subset E_{q,0}(K)$ by taking the series $X(u,q)$ modulo $\mathfrak{M}$

$$X(u,q) \equiv \frac{u}{(1-u)^2} \not\equiv 0 \pmod{\mathfrak{M}} \quad \text{for all } u \in R^*. \tag{4.85}$$

In order to prove the equivalence, we have a well-defined injective homomorphism on the quotient groups from the fact that $\phi(R_1^*) = E_{q,1}(K)$:

$$\mu : k^* \cong R^*/R_1^* \xrightarrow{\phi} E_{q,0}(K)/E_{q,1}(K) \cong E_{q,ns}(k) \tag{4.86}$$

$$u \mapsto \left(\frac{u}{(1-u)^2}, \frac{u^2}{(1-u)^3}\right). \tag{4.87}$$

This map μ is surjective, the inverse map is

$$(x, y) \mapsto \frac{y^2}{x^3}. \tag{4.88}$$

So, the map μ is an isomorphism.
We can then write the following commutative diagram:

$$\begin{array}{ccccccccc} 1 & \longrightarrow & R_1^* & \longrightarrow & R^* & \longrightarrow & k^* & \longrightarrow & 1 \\ & & \downarrow\sim & & \downarrow \phi & & \downarrow\sim & & \\ 0 & \longrightarrow & E_{q,1}(K) & \longrightarrow & E_{q,0} & \longrightarrow & \tilde{E}_{q,ns}(k) & \longrightarrow & 0\,. \end{array}$$

The diagram implies that the map $\phi : R^* \mapsto E_{q,0}(K)$ is an isomorphism.
It remains to prove that the injective homomorphism $\phi : K^*/R^*q^{\mathbb{Z}} \mapsto E_q(K)/E_{q,0}(K)$ is surjective.
The group on the left is easy to describe, since the map

$$K^*/R^*q^{\mathbb{Z}} \longmapsto \mathbb{Z}/ord_v(q)\mathbb{Z} \tag{4.89}$$

$$u \longmapsto ord_v(u) \tag{4.90}$$

is clearly an isomorphism.
Therefore, if we prove the following lemma, we can prove the surjectivity.

Lemma 4.2.6.

$$\#E_q(K)/E_{q,0}(K) \leq ord_v(q) \tag{4.91}$$

[7, lemma V.4.1] We divide E_q into subsets and show that those are cosets whose number is not greater than $ord_v(q)$.

Lemma 4.2.7. *Let $P = (x, y) \in E_q(K)$. The following conditions on points are equivalent:*

1. $P \in E_{q,0}(K), |x| \geq 1, |y| \geq 1$;
2. $|x| \geq 1$;
3. $|y| \geq 1$.

The proof is given in [7, Lemma V.4.1]. Then, we partition the points of $E_q(K)$ not in $E_{q,0}(K)$.

Lemma 4.2.8. *Let $P = (x, y) \in E_q(K)/E_{q,0}(K)$. Then exactly one of the following three conditions is true:*

1. $1 > |y| > |x + y|$ *in which case* $|y| > |q|^{\frac{1}{2}}$;
2. $1 > |x + y| > |Y|$, *in which case* $|x + y| > |q|^{\frac{1}{2}}$;
3. $|y| = |x + y| = |q|^{\frac{1}{2}}$.

The proof is given in [7, Lemma V.4.1.2]. the previous 2 lemmas allow us to divide $E_q(K)$ into the following subsets:

$$E_{q,0}(K) = \{(x, y) \in E_q(K) : |x| \geq 1 \text{ or } |y| \geq 1\}; \tag{4.92}$$
$$U_n = \{(x, y) \in E_q(K) : |\pi|^n = |y| > |x + y|\}; \tag{4.93}$$
$$V_n = \{(x, y) \in E_q(K) : |\pi|^n = |x + y| > |y|\}; \tag{4.94}$$
$$W = \{(x, y) \in E_q(K) : |y| = |x + y| = |q|^{\frac{1}{2}}\}. \tag{4.95}$$
$$\tag{4.96}$$

Then, we study the different subsets: U_n and V_n are empty if $n \geq ord_v(q)$ $W = 0$ if $ord_v(q)$ is odd, so $E_q(K)$ is the union

$$E_q(K) = E_{q,0}(K) \cup W \bigcup_{1 \leq n < \frac{1}{2} ord_v(q)} (U_n \cup V_n). \tag{4.97}$$

Then $E_q(K)$ is divided into (at most) $ord_v(q)$ pieces.
To finish this, we prove that these subsets are the cosets of $E_{q,0}(K)$ in $E_q(K)$. This will not be shown; it is done by proving that 2 points are in the same subset if and only if they are in the same coset. This is simply a computationally long proof as found in [7, Lemma V.4.1.4] □

4.3 Uniformisation theorem

In summary, we have shown that for any $K/\mathbb{Q}_p$ and any $q \in K^*$ with $|q| < 1$, there is an isomorphism between the quotient group $K^*/q^{\mathbb{Z}}$ and an elliptic curve $E_q(K)$.
In an analogous situation over complex numbers, we know (*LId*) that every elliptic curve $E/\mathbb{C}$ is isomorphic to E_q for some $q \in \mathbb{C}^*$.
On K however we have the j invariant for $E_q(K)$ as

$$|j(E_q)| = \frac{1}{q} + 744 + 196884q + \cdots = \frac{1}{|q|} > 1. \tag{4.98}$$

Therefore, not all elliptic curves over K can be isomorphic to an E_q.
We already know that $|j(E)| > 1$ is a necessary condition, and we prove that it is also sufficient.

Lemma 4.3.1. *Let $a \in \overline{\mathbb{Q}_p}$ be an element with $|\alpha| > 1$. Then, there is a unique $q \in \mathbb{Q}_p(\alpha)^*$; with $|q| < 1$ such that $j(E_q) = \alpha$.*

Proof. The j-invariant of E_q is given by the series 4.98, which we write as

$$j(q) = \frac{1 + 744q + 196884q^2 + \dots}{q}. \tag{4.99}$$

The reciprocal of this series, which we will call $f(q)$, is given by the formula

$$f(q) = \frac{1}{j(q)} = \frac{q}{1 + 744q + 196884q^2 + \dots} \tag{4.100}$$

$$= q - 744q^2 + 356652q^3 - \dots \in \mathbb{Z}[q]. \tag{4.101}$$

Applying lemma 4.2.5 to the series f, we get a series $g(q) = q + ... \in \mathbb{Z}[q]$ such that $g(f(q) = q$ as formal power series in $\mathbb{Z}[q]$. Since $g(q)$ has integer coefficients and leading term q, it will converge if we evaluate it at any element $\beta \in \mathbb{Q}_p$ of absolute value less than 1. $g(q)$ satisfy also $|g(\beta)| = |\beta|$. In particular, since $|\alpha| > 1$ we find that

$$q = g\left(\frac{1}{\alpha}\right) \in \mathbb{Q}_p(\alpha) \tag{4.102}$$

satisfies $0 < |q| = |\frac{1}{\alpha}| < 1$ and $\frac{1}{j(q)} = f(q) = f\left(g\left(\frac{1}{\alpha}\right)\right) = \frac{1}{\alpha}$. Hence $j(q) = \alpha$ as desired. This proves the existence part of theorem 4.3.1. In order to prove uniqueness, we suppose that $j(q) = j(q')$ with $|q| < 1$ and $|q'| < 1$. Then $f(q) = f(q')$.So,

$$0 = |f(q) - f(q')| = |q - q'| \cdot |1 - 744(q + q') + 356652(q^2 + qq' + q'^2) + \dots| = |q - q'|. \tag{4.103}$$

Therefore $q = q'$. □

Prior to demonstrating the p-adic uniformisation theorem, we introduce an invariant that is beneficial for examining the twists of a curve.

Lemma 4.3.2. *Let E/K be an elliptic curve defined over a field of characteristic not equal to 2 or 3, and choose a Weierstrass equation*

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \tag{4.104}$$

for E/K. Let c_4 and c_6 be the usual quantities associated to this equation. Assuming that $j(E) \neq 0, 1728$, we define

$$\gamma(E) = -\frac{c_4}{c_6} \in K^*/K^{2*}. \tag{4.105}$$

Where c_4, c_6 are defined in 1.1.3.
So, now we prove the following facts:

1. *$\gamma(E/K)$ is well-defined as an element of K^*/K^{*2}, independent of the choice of the Weierstrass equation for E/K.*

2. *Let E'/K be another elliptic curve with $j(E') \neq 0, 1728$. Then E and E' are isomorphic over K if and only if $j(E) = j(E')$ and $\gamma(E/K) = \gamma(E'/K)$.*

3. *Let E/K and E'/K be elliptic curves with $j(E') = j(E) \neq 0, 1728$ and suppose that $\gamma(E/K) \neq \gamma(E'/K)$, so*

$$L = K\left(\sqrt{\frac{\gamma(E/K)}{\gamma(E'/K)}}\right) \tag{4.106}$$

is a quadratic extension of K. Let

$$\chi : G_{\overline{K}/K} \longmapsto G_{L/K} \longmapsto \pm 1 \tag{4.107}$$

be the quadratic character associated to L/K. Now, we consider that there is an isomorphism

$$\psi : E \mapsto E' \tag{4.108}$$

with the property

$$\psi((P^{\sigma}) = \chi(\sigma)\psi(P) \text{ for all } \sigma \in G_{\overline{K}/K} \text{ and all } P \in E(K). \tag{4.109}$$

Proof. We prove 1. The condition $j(E) \neq 0, 1728$ is equivalent to $c_4 \neq 0$ and $c_6 \neq 0$, so $\gamma(E/K)$ exists. Then the coefficients of E and E' are related to the following $u^4 c_4' = c_4$ and $u^6 c_6 = c_6$ for some $u \in K^*$. Therefore,

$$\frac{c_4'}{c_6'} = u^2 \frac{c_4}{c_6} \pmod{K^{*2}} \tag{4.110}$$

which proves that $\gamma(E/K)$ is independent of the chosen Weierstrass equation. We now prove 2. If E and E' are isomorphic over K, then 1.1.4 asserts that $j(E) = j(E')$. Moreover, because the Weierstrass equations for E and E' describe the same elliptic curve over K, it follows from 1 that $\gamma(E/K) = \gamma(E'/K)$. Conversely, suppose that $j(E) = j(E')$ and $\gamma(E/K) = \gamma(E'/K)$. We consider the case in which $char(K) \neq 2, 3$, so, we can find Weierstrass equations for E, E' over K of the form

$$E : y^2 = x^3 + Ax + B, E' : y^2 = x^3 + A'x + B', \tag{4.111}$$

with $A, B, A', B' \in K$. Given our assumption

$$\gamma(E/K) = \gamma(E'/K) \tag{4.112}$$

Since $j(E) = 1728\frac{4A^3}{4A^3+27B^2}$, $c_4 = -48A$ and $c_6 = -864B$; the fact that $j(E) = j(E') \neq 0, 1728$ means that

$$\frac{2A}{B} \equiv \frac{2A'}{B'} \pmod{K^{*2}} \tag{4.113}$$

and so we find $t \in K^*$ such that $AB' = t^2 A'B$. Now, we can create the map

$$E \longmapsto E' \tag{4.114}$$
$$(x, y) \longmapsto (t^2 x, t^3 y) \tag{4.115}$$

that is an isomorphism. We now prove 3. With the same condition on j as before, we obtain $A^3 B'^2 = A'^2 B^3$. Then,

$$t = \sqrt{\frac{c_4 c_6'}{c_4' c_6}} = \sqrt{\frac{AB'}{A'B}} \text{ so } t^2 \equiv \frac{\gamma(E/K)}{\gamma(E'/K)} \pmod{K^{*2}}. \tag{4.116}$$

Since $\gamma(E/K) \neq \gamma((E'/K)$, we know that $L = K(t)$ is a quadratic extension of K then the map is an isomorphism

$$\psi : E \longmapsto E' \tag{4.117}$$
$$(x, y) \longmapsto (t^2 x, t^3 y). \tag{4.118}$$

Then, $\forall \sigma \in G_{\overline{K}/K}$, we know that $t^\sigma = \chi(\sigma) t$. So, for $P = (x, y) \in E(K)$ we have:

$$\begin{aligned} \psi(P)^\sigma = \psi(x, y)^\sigma &= (t^2 x, t^3 y)^\sigma = (\chi(\sigma)^2 t^2 x^\sigma, \chi(\sigma)^3 t^3 y^\sigma) \\ &= (t^2 x^\sigma, \chi(\sigma) t^3 y^\sigma) = \chi(\sigma)(t^2 x^\sigma, t^3 y^\sigma) = \chi(\sigma)\psi(P^\sigma). \end{aligned} \tag{4.119}$$

The above equation proves the lemma. □

We are now prepared to prove Tate's p-adic uniformisation theorem, which is applicable to all elliptic curves with an absolute value of the j-invariant exceeding 1.

Remark 4.3.3. The following theorem is also proven in [5, chapter II.5] with an analytic approach. The easiest way to generalise 4.3.4 is to consider the topic of rigid analysis through the uniformisation of Mumford curves. The proof on this line is proved in [2, Chapther 9.7].

Theorem 4.3.4. *(Tate) Let K be a p-adic field, let E/K be an elliptic curve with $|j(E)| > 1$, and let $\gamma(E/K) \in K^*/K^2*$.*

1. *There is a unique $q \in K^*$ with $|q| < 1$ such that E is isomorphic over $\overline{K}$ to the Tate curve E_q .*
2. *Let q be chosen as in 1. Then the following three conditions are equivalent:*
   - *(a) E is isomorphic to E_q over K.*
   - *(b) $\gamma(E/K) = 1$.*
   - *(c) E has split multiplicative reduction.*

Proof. We now prove 1. From lemma 4.3.1, $\exists! q \in K^*$ with $|q| < 1$ such that $j(E_q) = j(E)$ and as they are both elliptic curves $E_q \cong E$ over K. This comes from theorem 1.1.4-3 that E_q is isomorphic to $E(K)$, which are then isomorphic over $\overline{K}$.
We now prove 2. According to 4.3.2 we know that E is isomorphic to E_q over K if and only if $j(E) = j(E_q)$ and ,

$$\gamma(E/K) = \gamma(E_q/K). \tag{4.120}$$

So, in order to prove that 2a and 2b are equivalent, we must show that $\gamma(E_q/K) = 1$. With 4.2.2 we find that the c_4 and c_6 values associated with the Tate curve are:

$$c_4(q) = 1 - 48a_4(q) = 1 + 240s_3(q), \tag{4.121}$$
$$c_6(q) = -1 + 72a_4(q) - 864a_6(q) = -1 + 504s_5(q). \tag{4.122}$$

Consequently, the γ-invariant of E_q/K is equal.
In order to prove that $\gamma(E_q/K)$ is a square, we use the following lemma, which implies that $c_4(q)$ and $c_6(q)$ are themselves squares in K.

Lemma 4.3.5. *Let $\alpha \in K^*$ be with $|\alpha| < 1$. Then $1 + 4\alpha$ is a square in K.*

Proof. We consider the binomial coefficients:

$$\binom{-1/2}{n} = \frac{\left(-\frac{1}{2}\right)\cdot\left(-\frac{3}{2}\right)\cdot\left(-\frac{5}{2}\right)\cdots\left(-\frac{2n-1}{2}\right)}{n!} = \frac{(-1)^n}{4^n}\binom{2n}{n} \tag{4.123}$$

is an integer divided by 4^n. Then,

$$(1+4\alpha)^{-\frac{1}{2}} = \sum_{n=0}^{\infty}\binom{-1/2}{n}(4\alpha)^n = \sum_{n=0}^{\infty}(-1)^n\binom{2n}{n}\alpha^n. \tag{4.124}$$

Thus, the coefficients of the previous series are integers and the series converges in K. Hence $(1 + 4\alpha)^{-1}$ is a square in K and also $1 + 4\alpha$ is a square. □

Let us observe that since $|a_4(q)| = |a_6(q)| = |q| < 1$, the equation of the simplified curve E_q is evidently split multiplicative reduction. This shows that 2a leads to 2c. Conversely, assume that E has split multiplicative reduction. Now, we demonstrate that $\gamma(E/K) = 1$, thus proving that 2c results in 2b. We consider a minimal Weierstrass equation for E over k the residue field. As seen in the previous chapter, we assume that the singular point is on $(0, 0)$ that lies on the curve and is singular modulo $\mathfrak{M}$. Then

$$a_3 \equiv a_4 \equiv a_6 \equiv 0 \pmod{\mathfrak{M}} \tag{4.125}$$

and hence we have that

$$b_4 = a_1a_3 + 2a_4 \equiv 0 \pmod{\mathfrak{M}} \text{ and } c_4 = b_2^2 - 24b_4 \equiv b_2^2 \pmod{\mathfrak{M}}. \tag{4.126}$$

From 3.3.4, E has multiplicative reduction implies that $c_4 \not\equiv 0 \pmod{\mathfrak{M}}$, so we see that $b_2 \not\equiv 0 \pmod{\mathfrak{M}}$. Therefore, b_2 is a unit and $|b_2| = 1$. Hence,

$$\gamma(E/K) = -\frac{c_4}{c_6} = \frac{1}{b_2} \cdot \left(\frac{1 - 24\dfrac{b_4}{b_2^2}}{1 - 36\dfrac{b_4}{b_2^2} + 216\dfrac{b_6}{b_2^3}} \right) \pmod{K^{*2}}. \tag{4.127}$$

Using the previous lemma, to the numerator and denominator of the fraction in the brackets on the right-hand side of this equation, we find that both the numerator and the denominator are squares and are therefore in K^{*2}. Thus,

$$\gamma(E/K) \equiv \frac{1}{b_2} \equiv b_2 \pmod{K^{*2}} \tag{4.128}$$

It remains to show that if the multiplicative reduction of E is split, which is equivalent to b_2 is a square in K^*. The reduction of E is

$$\tilde{E} : y^2 + \tilde{a}_1 xy = x^3 + \tilde{a}_2 x^2 \tag{4.129}$$

We factor the polynomial

$$y^2 + \tilde{a}_1 xy - \tilde{a}_2 x^2 = (y - \tilde{\alpha}x)(y - \tilde{\beta}x). \tag{4.130}$$

The fact that E has multiplicative reduction means that E has a node, so $\tilde{\alpha} \neq \tilde{\beta}$ and the fact that the reduction is split means that $\tilde{\alpha}, \tilde{\beta}$ are actually in the residue field k, rather than in a quadratic extension. For more notions, look back at 3.3.4. It follows from Hensel's lemma that $\tilde{\alpha}, \tilde{\beta}$ lift uniquely to elements $\alpha, \beta \in K$ such that

$$y^2 + \tilde{a}_1 xy - \tilde{a}_2 x^2 = (y - \alpha x)(y - \beta x). \tag{4.131}$$

Hence,

$$b_2 = a_1 + 4a_2 = (-\alpha - \beta)^2 + 4(-\alpha(\beta) = (\alpha - \beta)^2 \in K^{*2}, \tag{4.132}$$

so $\gamma(E/K) \equiv b_2 \equiv 1 \pmod{K^{*2}}$. We have now proven 2*b* $\implies$ 2*a* $\implies$ 2*c* $\implies$ 2*b*, which completes the proof of the Theorem. □

Suppose that we have an elliptic curve E/K as in the precedent Theorem with invariant $\gamma((E/K) \neq 1$. If we let $L = K(\sqrt{\gamma((E/K)})$, which is well-defined, since $\gamma((E/K)$ is defined up to squares in K, it becomes clear that $\gamma((E/L) = 1$. Applying 4.3.4 to E/L, we find that E is isomorphic to E_q over L, so

$$E(L) \cong E_q(L) \cong L^*/q^{\mathbb{Z}} \tag{4.133}$$

We will now describe $E(K)$ in terms of this identification.

Lemma 4.3.6. *With notation as in the preceding paragraph,*

$$E(K) \cong u \in L^*/q^{\mathbb{Z}} : N_K^L(u) \in q^{\mathbb{Z}}/q^{2\mathbb{Z}} \tag{4.134}$$

where N is norm map $|\cdot|$ *which is a homomorphism*

$$N_K^L : L^*/q^{\mathbb{Z}} \mapsto K^*/q^{2\mathbb{Z}}. \tag{4.135}$$

and $N(u)$ *is well-defined modulo* $q^{2\mathbb{Z}}$.

Proof. First, we observe that applying the 4.3.2 to E and E_q, there is an isomorphism $\psi : E_q(\overline{K}) \mapsto E(\overline{K})$ satisfying $\psi(P^\sigma) = \chi(\alpha)\psi(P)^\sigma$ for all $\alpha \in G_{\overline{K}/K}$, where

$$\chi : G_{\overline{K}/K} - > G_{L/K} - > \pm 1 \tag{4.136}$$

is the quadratic character associated to L/K. On the other hand, the isomorphism

$$\phi : \overline{K} * /q^{\mathbb{Z}} \longmapsto E_q(K) \tag{4.137}$$

is defined over K, which means that $\phi(P\sigma) = \phi(P)^\sigma$. We look at the composition

$$L^*/q^{\mathbb{Z}} \overset{\phi}{\leftarrow} E_q(L) \overset{\psi}{\leftarrow} E(L). \tag{4.138}$$

We know from above is an isomorphism of groups. Let $\tau \in G_{\overline{K}/K}$ be an element with $\chi(\tau) = -1$, so τ represents the non-trivial element in $G_{L/K}$ Then for any $u \in L^*$,

$$\begin{aligned}
(\psi \circ \phi)(u) \in E(K) &\iff \psi(\phi(u)^\tau = \psi(\phi(u) && (4.139)\\
&\iff -\psi(\phi(u^\tau)) = \psi(\phi(u) \text{ since } \chi(\tau) = -1 && (4.140)\\
&\iff \psi(\phi(u^{-\tau})) = \psi(\phi(u) && (4.141)\\
&\quad \text{since } -\psi(P) = \psi(-P) \text{ and } -\psi(u) = \psi(u^{-1}) && (4.142)\\
&\iff u^{-\tau} \equiv u \pmod{q^{\mathbb{Z}}}. && (4.143)\\
& && (4.144)
\end{aligned}$$

Since ψ and ϕ are isomorphisms $u^{1+\tau} \in q^{\mathbb{Z}}$ Since $u^{1+\tau} = N_k^L(u)$, this completes the proof of the corollary. □

Bibliography

[1] Harald Baier. "How to compute the coefficients of the elliptic modular function ." eng. In: *Experimental Mathematics* 12.1 (2003), pp. 115–121. URL: http://eudml.org/doc/51095.

[2] Siegfried Bosch et al. *Non-Archimedean analysis : a systematic approach to rigid analytic geometry /*. eng. Grundlehren der mathematischen Wissenschaften. Berlin: Springer, 1984. ISBN: 0387125469.

[3] Peter Bruin. "Formal Groups/ seminar notes". eng. 2006. URL: https://pub.math.leidenuniv.nl/~bruinpj/formal-groups.pdf.

[4] Serge Lang. *Elliptic functions*. eng. 2. ed. Graduate texts in mathematics. New York [etc: Springer, 1987. ISBN: 0387965084.

[5] Alain Robert, Beno Eckmann, and A. Oold. *Elliptic curves : notes from postgraduate lectures given in Lausanne 1971/72*. eng. 1st ed. 1973. Lecture Notes in Mathematics, 326. Berlin, Germany ; Springer-Verlag, 1986. ISBN: 3-540-46916-8.

[6] Peter Roquette. *Analytic theory of elliptic functions over local fields*. eng. Hamburger mathematische einzelschriften. Gottingen: Vandenhoeck & Ruprecht, 1970.

[7] Joseph H. Silverman. *Advanced topics in the arithmetic of elliptic curves*. eng. Graduate texts in mathematics. New York [etc: Springer, 1994. ISBN: 0387943250.

[8] Joseph H. Silverman. *The arithmetic of elliptic curves*. eng. 2. ed. Graduate texts in mathematics. New York: Springer, 2009. ISBN: 9780387094939.

[9] John Stillwell. "Elliptic Curves". In: *The American Mathematical Monthly* 102.9 (1995), pp. 831–837. ISSN: 00029890, 19300972. URL: http://www.jstor.org/stable/2974515.

[10] Chris Williams. "MA4M3 Local Fields Lecture Notes". eng. 2003. URL: https://warwick.ac.uk/fac/sci/maths/people/staff/cwilliams/lecturenotes/lecturenotes.pdf.