A review of non-archimedean elliptic functions, John Tate

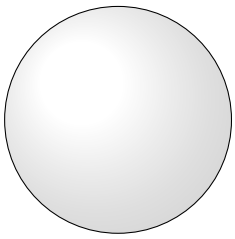
Salim Alloun

I present an article of Tate **[1]** which is composed of two parts. The first is an old manuscript dating from 1959 containing his first proof of that for certain elliptic curves E_t we have $E_t(k) \simeq k^\times/t^{\mathbb{Z}}$. The second part dwells into theta functions, isogenies, torsion points and Serre's isogeny theorem. I will only mention the things I found interesting especially as a complement to what we have done in Thuillier's course.

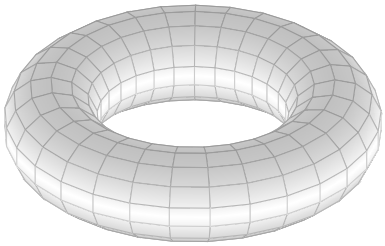
1 Introduction

John Tate engaged himself in the work of uniformizing the elliptic curves over non-archimedean fields. The uniformization of curves over $\mathbb{C}$ had already been done at his time, with a concrete classification. More precisely, let X be an algebraic smooth curve over $\mathbb{C}$ such that $X(\mathbb{C})$ is compact then $X(\mathbb{C})$ is an orientable compact surface with a topological invariant which is the number of holes in that surface (called the *genus* g) :

- $\underline{g = 0}$: $X(\mathbb{C}) \simeq \mathbb{S}^2$ and therefore is simply connected, its topological universal covering is itself.



- $\underline{g = 1}$: The universal covering of $X(\mathbb{C})$ is $\mathbb{C}$ and there exists a lattice Λ of $\mathbb{C}$ such that $X(\mathbb{C}) \simeq \mathbb{C}/\Lambda$.



- $\underline{g \geqslant 2}$: The universal covering of $X(\mathbb{C})$ is $\mathfrak{h}$, and $X(\mathbb{C}) \simeq \Gamma\backslash\mathfrak{h}$ where Γ is a torsion-free discrete subgroup of $\mathrm{PSL}_2(\mathbb{R})$.

In general, the curves of genus 1 are the first non-trivial curves (as the genus 0 curves are all isomorphic as algebraic curves to the projective line) and furthermore they are abelian varieties meaning in this context curves together with a compatible structure of an abelian group. The genus 1 curves are called *elliptic curves*. However the genus can actually be algebraically defined for any curve (via the Riemann-Roch theorem), and over any field k an elliptic curve is a curve defined in $\mathbb{P}^2_k$ by this kind of projective equation :

$$ZY^2 + a_1XZY + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3 \qquad (1)$$

The interesting thing to see here is that for an elliptic curve E over $\mathbb{C}$ we can write $E(\mathbb{C}) \simeq \mathbb{C}/\Lambda$ for a certain lattice Λ, and up to changing $\mathbb{C}$ via an homotethy I can chose $(1, \tau)$ as a basis of Λ. In fact the universal covering of $E(\mathbb{C})$ is a function $f : \mathbb{C} \longrightarrow E(\mathbb{C})$ that we can write (up to changing the equation (1) via affine transformations) in the following way :

$$f(z) = (\wp(z) : \wp'(z) : 1)$$

and $\wp$ is a meromorphic function invariant by $\Lambda = \mathbb{Z} \oplus \mathbb{Z}\tau$. The functions being periodic regarding two real directions are called *elliptic functions* and $\wp$ is called the Weierstraß function of parameter τ (or parameter Λ). So in particular being periodic regarding 1 implies that f can be factorized by an exponential and so we can see with $t = \exp(2i\pi\tau)$ that

$$E(\mathbb{C}) \simeq \mathbb{C}^\times / t^{\mathbb{Z}}$$

Given the fact there is no counterpart to exponential in the non-archimedean world, John Tate understood that we should stick to the hope that we can describe elliptic curves over k a non-archimedean field by $k^\times/t^{\mathbb{Z}}$, for a suitable t. This hope is even more tangible considering the following. With the change of variable $z \mapsto w = \exp(2i\pi z)$, Tate gives the computation

$$x(w) := \wp(z) - \frac{1}{12} = \frac{w}{(1-w)^2} + \sum_{m=1}^{\infty} \left(\frac{t^m w}{(1-t^m w)^2} + \frac{t^m w^{-1}}{(1-t^m w^{-1})^2} - 2\frac{t^m}{(1-t^m)^2} \right)$$

As a power series the right-hand term has all of its coefficients in $\mathbb{Z}[[t]]$ and so if $|t| < 1$ then it can define a function on $k^\times$(for the variable w, the relevant one in this context anyway) . The same goes for the coefficients in (1), they can be expressed with power series which make sense in the non-archimedean world. Plus we have the equation

$$x(w) = x(tw) = x(w^{-1})$$

Finally, Tate use y a power series which is a counterpart to the derivative $\wp'$, and is found via the equation

$$(\wp'(z) \approx) \quad w\frac{\mathrm{d}x}{\mathrm{d}w}(w) = x(w) + 2y(w)$$

but [1] defined by

$$y(w) := \frac{w^2}{(1-w)^3} + \sum_{m=1}^{\infty} \left(\frac{t^{2m} w^2}{(1-t^m w)^3} - \frac{t^m w^{-1}}{(1-t^m w^{-1})^3} + \frac{t^m}{(1-t^m)^2} \right)$$

1. 2 can be zero...

2 Proof in the Old Manuscript

In the course *Rigid geometry of algebraic curves* given by Amaury Thuillier, we saw a proof that such description exists when the j-invariant of E is such that $|j| < 1$. The proof has been given in the language of Berkovich. In the paper of John Tate, he proves it with the point of view of abelian varieties.

Let k be a non-archimedean complete field. Tate gives an appropriate affine equation :

$$y^2 + xy = x^3 - b_2 x - b_3$$

where $b_2, b_3 \in \mathbb{Z}[[t]]$ verify

$$b_2 = 5\sum_{n=1}^{\infty} \frac{n^3 t^n}{1-t^n} \quad b_3 = \sum_{n=1}^{\infty} \frac{7n^5 + 5n^3}{12} \frac{t^n}{1-t^n}$$

to define E_t an elliptic curve over k, where one should add (∞, ∞), noted by O, the neutral element for the group law of E_t. As said before, power series with coefficients in $\mathbb{Z}$ makes sense in k and the formula in the complex world is still true

$$j(E_t) = t^{-1}(1 + 744t + 196884t^2 + \ldots)$$

If k is algebraically closed, given that j gives the isomorphism class of an elliptic curve, then any elliptic curve over k such that $|j| > 1$ is isomorphic to a curve E_t, via the inverse formal series :

$$t = j^{-1}(1 + 744j^{-1} + 750420j^{-2} + \ldots)$$

Theorem 2.1. *(Tate) There exists a group morphism $k^\times \longrightarrow E_t(k)$ with kernel equal to $t^{\mathbb{Z}}$.*

Proof. The idea is to define a map φ such that $\varphi(w) = (x(w), y(w))$ if $w \notin t^{\mathbb{Z}}$ and O if $w \in t^{\mathbb{Z}}$.[2] The whole proof is to show that φ is indeed a group morphism (Lemma 1) and that it is surjective (Lemma 2 and 3). For this Tate use the algebraic equations defining the group law. □

3 Theta functions

I rapidly mention the principal ideas. As Poincaré in the complex case searched fuchsian functions (meaning invariant by a fuchsian group) as quotient of theta functions of same degree, here elliptic functions are also described as quotient of theta functions. It enables us to see more clearly the fact that y is derivative of x, because indeed Tate writes

$$x = D\zeta \quad \text{and} \quad y = D_2\zeta$$

where ζ is a meromorphic function coming from a kind of theta function, $D = w\frac{\mathrm{d}}{\mathrm{d}w}(w)$ (differential operator of degree 1) and $D_2 = \frac{1}{2}(D^2 - D)$ (differential operator of degree 2).

2. The invariance by t makes the crucial set of definition to be an annulus so in fact it is the same idea with what we have done with Thuillier.

4 Isogenies

Let C be the completion of an algebraic closure of k. Then C is algebraically closed (see [4], 4.4.2).

Definition 4.1. *(See [2]) Let $t_1, t_2 \in k^\times$ such that $|t_1|, |t_2| < 1$. An* isogeny *is a non-trivial morphism of algebraic curves $E_{t_1} \longrightarrow E_{t_2}$ sending O to O [3], non-trivial in the sense that the image should have at least another point than O. In [2], it is shown that those arrows are in fact group morphisms and an isogeny is necessarily surjective. We say that two elliptic curves are* isogenous *if there is an isgoeny between them.*

We say that t_1 and t_2 are *commensurable* if there exists non-zero $m, n \in \mathbb{Z}$ such that $t_2^m = t_1^n$. Suppose they are. Then $x \mapsto x^n (\bmod t_2)$ from $C^\times$ to $C^\times/t_2^{\mathbb{Z}}$ factorizes through $t_1^{\mathbb{Z}}$, and induces an isogeny

$$\alpha_{m,n} : E_{t_1}(C) \longrightarrow E_{t_2}(C)$$

Commensurable or not we can always define $\alpha_{0,0}$ which is the trivial group morphism.

Theorem 4.1. *(Tate) The map $\alpha_{m,n}$ is a covering of degree $|mn|$ and there is a bijection*

$$\mathrm{Hom}_C(E_{t_1}, E_{t_2}) \simeq \{(m,n) \in \mathbb{Z} \times \mathbb{Z}, t_2^m = t_1^n\}$$

In particular, E_{t_1} and E_{t_2} are isogenous if and only if t_1 and t_2 are commensurable.

Proof. The idea of the proof is to start from this commutative triangle :

$$\begin{array}{ccc} E_{t_1} & \xrightarrow{\alpha_{1,n}} & E_t \\ & \searrow^{\alpha_{m,n}} & \downarrow{\scriptstyle \alpha_{m,1}} \\ & & E_{t_2} \end{array}$$

where $t = t_1^m = t_2^n$. The extension of meromorphic function fields $\mathcal{M}(E_t)|\mathcal{M}(E_{t_2})$ is Galois generated by the translation by t_2 which is of order $|m|$, since the elements of $\mathcal{M}(E_t)$ are functions on $C^\times$ invariant by $t = t_2^m$. So $\alpha_{m,1}$ is of degree $|m|$ and by duality we have that $\alpha_{1,m}$ is of degree $|m|$.

The field C being algebraically closed, Tate asserts that an isogeny is the product of isogenies of prime degree. Then one has to show that a morphism $E_t \longrightarrow E_{t'}$ of prime degree p is of the form $\alpha_{p,1}$ or $\alpha_{p,1}$. Since $|j| > 1$ the curve E_t is "generic" meaning that its bijective isogenies are ± 1, and so up to sign an isogeny is determined by its kernel. We have the formula $\alpha_{-m,-n} = -\alpha_{m,n}$, so it suffices to look at the finite subgroups-schemes of E_t of order p.
$\underline{\mathrm{char}(C) \neq p}$: There is only one subgroup of order p in C^*, it is composed of the p-th roots of unity and it is a affine scheme with algebra $C[X]/(X^p - 1)$. In the quotient $C^*/t^{\mathbb{Z}}$, given that C is algebraically closed there is also the subgroup of order p composed of the p-th root of t (algebra = $C[X]/(X^p - t)$). Finally we get the two possible kernels, respectively of $\alpha_{1,p}$ and of $\alpha_{p,1}$.
$\underline{\mathrm{char}(C) = p}$: $\alpha_{1,p} : E_t \longrightarrow E_{t^p}$ and $\alpha_{p,1} : E_t \longrightarrow E_{t^{1/p}}$ are the so-called Frobenius and Verschiebung operator with kernels respectively being μ_p and $\mathbb{Z}/p\mathbb{Z}$ (they are Cartier duals of one another). The multiplication by p in the abelian group $E_t(C)$ is $\alpha_{p,p}$ which is taking the p-th power in $C^\times/t^{\mathbb{Z}}$. It is of degree p^2 so the kernel is of order p^2. Therefore there are two subgroups-schemes of order p. But μ_p is not isomorphic to $\mathbb{Z}/p\mathbb{Z}$ so here are the two subgroups.

□

3. Here the marked points of E_{t_1} and E_{t_2} are both O, in general we can chose other points...

Corollary 4.1. *For all* $0 < |t| < 1$, E_t *has only trivial endomorphisms, i.e.*

$$\mathrm{End}(E_t) := \mathrm{Hom}_k(E_t, E_t) = \mathrm{Hom}_C(E_t, E_t) \simeq \mathbb{Z}$$

Interpretation of the condition $|j| > 1$

Tate mentions a comment made by Serre about elliptic curves with complex multiplication (or CM-elliptic curves), i.e. curves with an endomorphism ring strictly bigger than $\mathbb{Z}$.

Corollary 4.2. *The* j*-invariant of a CM-elliptic curve* E *over a finite extension* $F|\mathbb{Q}$ *is an algebraic integer.*

Lemma 4.1. $x \in F$ *is an algebraic integer (over* $\mathbb{Z}$*) if and only if* $v(x) \geqslant 0$ *for all finite place* v *of* F*.*

Proof. If $f_{\min,\mathbb{Q},x} \in \mathbb{Z}[X]$ then by looking at its Newton polygon, we see that all of its slopes are non-positive and so x (being a root of P) has a non-negative valuation.

Now assume that $f = f_{\min,\mathbb{Q},x} \notin \mathbb{Z}[X]$. One of its coefficients has a negative p-adic valuation for at least one prime number p. So over $\mathbb{Q}_p$ there exists at least one point in the Newton polygon of f which is under the horizontal axis, and so there is at least one positive slope. x has therefore at least one Galois conjugate $y \in \overline{\mathbb{Q}}$ of negative valuation. Consider it to define a finite place v of F above p such that $v(x) < 0$. □

Proof. [Corollary 4.2.] Assume that j is not an algebraic integer. By the lemma there exists v such that $|j|_v > 1$. Then we have that $E \simeq E_t$ over F_v, for a $t \in F_v$. But there is at least one non-trivial endomorphism of E over $\mathbb{Q}$ and it induces a non-trivial endomorphism of E over F_v. *Contradiction.* □

Remark 4.1. *Corollary 4.2. has been proved in many ways, but this shows how fruitful is the idea of considering "being an algebraic integer over* $\mathbb{Z}$*" as a local property in the space of prime numbers.*

So here we see that in the moduli space of elliptic curves over k there is the set defined by $|j| > 1$ (parametrized by the variable t in the unit disk without 0) and the rest is more diverse with CM-curves playing the role of peculiar points.

Naive questions stemming from the article :

- Is there any exponential $k \longrightarrow k^\times$? If that's not the case (and I think it is not) : why ?
  In the case of non-archimedean field of characteristic $p > 0$, there is for example formulae who looks like the famous
  $$\frac{\zeta(2n)}{(2i\pi)^{2n}} \in \mathbb{Q}$$
  where one replace $2i\pi$ by an element ξ (defined modulo $\mathbb{F}_q^\times = \mathbb{F}_q[T]^\times$ like $2i\pi$ is defined modulo $\{\pm 1\} = \mathbb{Z}^\times$ because i can be changed with $-i$) See [3].
- Is there a precise description of the subset $|j| \leqslant 1$ inside the moduli space of elliptic curves ?

References.

[1] : Tate, J. (1997). A review of non-archimedean elliptic functions.

[2] : Silverman, J. (2009). The arithmetic of elliptic curves (2nd ed., Graduate texts in mathematics 106).

[3] : Goss, D. (1998). Basic structures of function field arithmetic. Berlin Heidelberg : Springer.

[4] : Robba, & Christol. (1994). Équations différentielles p-adiques applications aux sommes exponentielles (Actualités mathématiques).