Tate Day
Tate Elliptic Curves and p-adic Uniformization

Shay Ben Moshe

16/12/2019

A detailed account of this topic is in [Sil11, see V.1-6]. A short introduction can be found on [Mie; Li].

1 Introduction to Elliptic Curves

There are various different perspectives, motivations and interesting aspects to elliptic curves. I will try give (or hint) some of them.

In high school we all learn about *lines* L and *quadratic curves* Q: circles/ellipses, parabolas and hyperbolas. These are the solutions to polynomials of the form $L : ay+bx+c = 0$, and degree 2 respectively. We are then naturally led to consider *cubic curves* E, that is solutions of polynomials $f(x, y)$ with $\deg f = 3$. Another interesting direction of generalization is to consider curves over fields or rings other then $\mathbb{R}$ or $\mathbb{C}$, such as $\mathbb{Q}$, $\mathbb{F}_p$ or $\mathbb{Z}_p$ (p-adics), and to look for solutions there, denoted $E(R) = \{x, y \in R \mid f(x, y) = R\}$. (To the algebro-geometric minded, we really mean $E = \operatorname{Spec} R[x, y]/f$.)

We note that some polynomials give singular curves, for example, $y^2 = x^2$ looks like the shape X, which has a node at the origin; and $y^2 = x^3$ looks like $\prec$, which has a cusp at the origin. We would like to restrict ourselves to smooth (non-singular) curves. Smooth cubic curves are called *elliptic curves*, and it turns out that (up to change of coordinates) any elliptic curve is given by $E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$, called the *Weierstrass equation* (where the a_i's need to satisfy some condition to ensure smoothness). Furthermore, away from characteristic $2, 3$ we can change coordinates further to $E : y^2 = x^3 + Ax + B$ (where $4A^3 + 27B^2 \neq 0$ to ensure smoothness).

1.1 Group Structure

An especially interesting and useful property of elliptic curves is that they admit an abelian group structure. To be precise, we need to add a point at ∞ (i.e. projectivize), usually denoted O, which serves as a 0 for the group structure. The group structure is determined as follows: take two points P, Q, connect them by a line, and look for the third intersection R, then $P + Q + R = O$. (Using this and $P + (-P) + O = O$ the structure is determined, though associativity is not obvious.)

It is worth noting that these operation are rational functions in the coordinates of P, Q, thus if they are in $E(K)$, then $P + Q$ is also in $E(K)$. That is, the set of K-points $E(K)$ is a group.

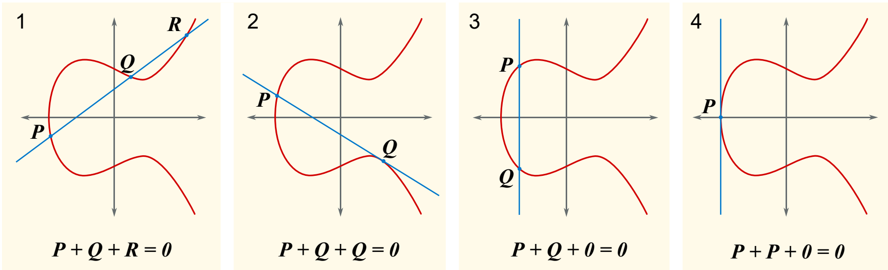

Figure 1: Addition on $E : y^2 = x^3 - x + 1$ over $\mathbb{R}$ (taken from Wikipedia)

2 Elliptic Curves over $\mathbb{C}$

Elliptic curves over $\mathbb{C}$, have a very special property: they admit analytic uniformization. Let Λ be a lattice in $\mathbb{C}$, (up to rotation and scaling) that is $\Lambda = \mathbb{Z} + \tau\mathbb{Z}$ for $\tau \in \mathbb{C} \setminus \mathbb{R}$. We can consider the group quotient $\mathbb{C}/\Lambda$, which looks like a (real) torus, though note that it is of complex dimension 1. An interesting observation is that this parameterizes an elliptic curve over $\mathbb{C}$ (as defined above). Define $\wp(z) = \frac{1}{z^2} + \sum_{\omega \in \Lambda, \omega \neq 0} \left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right)$ (which depends on Λ). Unfortunately I don't have time to motivate this definition, but it is worth noting that it converges outside Λ, and Λ-periodic, therefore, descends to a function $\mathbb{C}/\Lambda \to \mathbb{C} \cup \{\infty\}$ (where $[0]$ is mapped to ∞). Furthermore, the derivative $\wp'(z)$ satisfies the same properties. Remarkably, $\wp'(z)^2 = 4\wp(z)^3 - g_2\wp(z) - g_3$ for some $g_2, g_3 \in \mathbb{C}$ (which depend on Λ), i.e. the pair $(x, y) = (\wp(z), \wp'(z))$ solves the Weierstrass equation $E_\Lambda : y^2 = 4x^3 - g_2 x - g_3$. In fact, it turns out:

Theorem 1 (analytic uniformization [Sil09, see VI.3.6])**.** *The map* $\mathbb{C}/\Lambda \xrightarrow{(\wp(z), \wp'(z))} E_\Lambda(\mathbb{C})$ *(which sends the lattice points to O) is an isomorphism of Lie groups. Moreover, every elliptic curve $E/\mathbb{C}$ is isomorphic to some E_Λ.*

Remark 2. This isomorphism is *not* Galois equivariant, so it tell us nothing about the rational or real points of E.

This gives a whole new arsenal to study elliptic curves over $\mathbb{C}$. As an example, we can immediately deduce the structure of the torsion of the curve, namely describe the subgroup of n-torsion points i.e. $E[n] = \{P \in E(\mathbb{C}) \mid nP = O\}$. From the algebraic description this is not an easy task. However, using the model $\mathbb{C}/\Lambda$ it is immediate that the n-torsion points are $\frac{a}{n}1 + \frac{b}{n}\tau$, that is $E[n] \cong \mathbb{Z}/n \times \mathbb{Z}/n$.

3 p-adic Uniformization

We would like to do something similar in the p-adic situation, that is over $\mathbb{Q}_p$ (in fact this work over any p-adic field but for simplicity we stick to $\mathbb{Q}_p$). We could try and replace $\mathbb{C}/\Lambda$ by $\mathbb{Q}_p/\Lambda$, but this fails immediately as $\mathbb{Q}_p$ has no non-zero discrete subgroups.

Nevertheless, Tate had a clever trick. Let's revisit the case over $\mathbb{C}$. Consider the exponent function $\mathbb{C} \xrightarrow{e^{2\pi iz}} \mathbb{C}^\times$. This is clearly surjective homomorphism, with kernel $\mathbb{Z} \leq \mathbb{C}$, thus $\mathbb{C}/\mathbb{Z} \xrightarrow{\sim} \mathbb{C}^\times$. Recall the lattice $\Lambda = \mathbb{Z} + \tau\mathbb{Z}$, and denote $q = e^{2\pi i\tau}$, we get an isomorphism $\mathbb{C}/\Lambda \xrightarrow{\sim} \mathbb{C}^\times/q^{\mathbb{Z}}$ (where $q^{\mathbb{Z}} = \{\dots, q^{-1}, 1, q, q^2, \dots\}$). Further, we sat that $\mathbb{C}/\Lambda \xrightarrow{(\wp(z),\wp'(z))} E_\Lambda(\mathbb{C})$ is an isomorphism. We can combine the two isomorphisms to give an identification of $\mathbb{C}^\times/q^{\mathbb{Z}}$ with the points of E_Λ; explicitly , as $\wp(z)$ is Λ-periodic, we express it as a power series in $u = e^{2\pi iz}$ (essentially doing Fourier). It is convenient to do some simple (affine) change of variables (e.g. to get rid of $2\pi i$). Altogether we get functions $X(u), Y(u)$ which give an isomorphism $\mathbb{C}^\times/q^{\mathbb{Z}} \xrightarrow{(X(u),Y(u))} E_q(\mathbb{C})$. Here E_q is the elliptic curve after this change of coordinates, called *Tate elliptic curve*, given by $E_q : y^2 + xy = x^3 + a_4x + a_6$ where a_4, a_6 are power series in q. Remarkably, a_4, a_6, X, Y are power series in q with *integer coefficients.*

As we said, $\mathbb{Q}_p/\Lambda$ doesn't work, and we don't have an analogue for the exponent function. However, $\mathbb{Q}_p^\times$ has many discrete subgroups: let $q \in \mathbb{Q}_p^\times$ with $|q| < 1$, i.e. q is in the maximal ideal $\mathfrak{m} = p\mathbb{Z}_p$, then $\mathbb{Q}_p^\times/q^{\mathbb{Z}}$ is a good candidate. The power series for a_4, a_6, X, Y converge, using $|q| < 1$. Therefore, E_q can be defined over $\mathbb{Q}_p$ and we have maps $\mathbb{Q}_p^\times/q^{\mathbb{Z}} \xrightarrow{(X(u),Y(u))} E_q(\mathbb{Q}_p)$.

Theorem 3 (Tate [Sil11, see V.3.1])**.** *Let $q \in \mathbb{Q}_p^\times$ with $|q| < 1$. There is an isomorphism of (p-adic analytic) groups $\overline{\mathbb{Q}_p}^\times/q^{\mathbb{Z}} \xrightarrow{(X(u),Y(u))} E_q\left(\overline{\mathbb{Q}_p}\right)$. Furthermore, this isomorphism is Galois equivariant, in particular, for any algebraic extension $L/\mathbb{Q}_p$ we have an isomorphism $L^\times/q^{\mathbb{Z}} \xrightarrow{\sim} E_q(L)$.*

In the complex case, every elliptic curve $E/\mathbb{C}$ was isomorphic to some E_Λ. In contrast, *not* every elliptic curve $E/\mathbb{Q}_p$ is isomorphic to such E_q. One can see that the j-invariant (which we didn't define, but is an isomorphism invariant) satisfies $|j(E_q)| = \left|\frac{1}{q}\right| > 1$. Therefore, only $E/\mathbb{Q}_p$ with $|j(E)| > 1$ have a chance.

In addition, since $q \in \mathfrak{m} = p\mathbb{Z}_p$, we see that E_q is in fact defined over $\mathbb{Z}_p$ and not only over $\mathbb{Q}_p$. Thus we can define its reduction to $\mathbb{F}_p$ denoted $\tilde{E}_q$. This turns out to have a singular point, thus it is not an elliptic curve (bad reduction). The singularity type is a node, which implies that dropping it yields $\tilde{E}_{q,\mathrm{ns}} \cong \mathbb{G}_m$ (multiplicative reduction), and moreover the slopes of the tangents at the singularity are in $\mathbb{F}_p$ (split).

Theorem 4 (p-adic uniformization, Tate [Sil11, see V.5.3])**.** *Let $E/\mathbb{Q}_p$ be an elliptic curve such that $|j(E)| > 1$ then*

1. *there exists a* unique $q \in \mathbb{Q}_p^\times$ *with* $|q| < 1$ *such that* $E \cong E_q$ over $\overline{\mathbb{Q}_p}$,
2. *furthermore,* $E \cong E_q$ *over* $\mathbb{Q}_p$ *if and only if* E *has split multiplicative reduction.*

3.1 Application to Tate Modules

The Tate module of an elliptic curve is a very useful invariant. On the one had, many properties of the curve reflect in its Tate module, and on the other hand it provides an example of a Galois representation, i.e. a representation of $G = \mathrm{Gal}\left(\overline{\mathbb{Q}_p}/\mathbb{Q}_p\right)$.

Let ℓ be a prime, which may or may not be equal to p. We can consider the ℓ^n-*torsion* over the algebraic closure, $E[\ell^n] = \left\{P \in E\left(\overline{\mathbb{Q}_p}\right) \mid \ell^n P = O\right\}$. The G-action on $E\left(\overline{\mathbb{Q}_p}\right)$ restricts to an action on $E[\ell^n]$. To actually get the Tate module one need to take the limit over n, but for simplicity we shall work with $E[\ell^n]$ as the result is quite similar.

As a warm up, say instead of looking at E we looked at the multiplicative group $\mathbb{G}_m$, whose points are $\mathbb{G}_m\left(\overline{\mathbb{Q}_p}\right) = \overline{\mathbb{Q}_p}^\times$. Then $\mathbb{G}_m[\ell^n] = \left\{\zeta_{\ell^n}^k \mid 0 \leq k \leq \ell^n - 1\right\} \cong \mathbb{Z}/\ell^n$ where ζ_{ℓ^n} is a primitive root of unity. Furthermore, we have a Galois action. Namely, any element $g \in G$ sends ζ_{ℓ^n} to another primitive ℓ^n-th root of unity. Therefore we get that $g\zeta_{\ell^n} = \zeta_{\ell^n}^{\chi(g)}$ for some $\chi(g) \in (\mathbb{Z}/\ell^n)^\times$. So we get a homomorphism $\chi : G \to (\mathbb{Z}/\ell^n)^\times$ called the *cyclotomic character* (actually the cyclotomic character is the limit over n).

Now, say that $E = E_q$ is a Tate elliptic curve for some $|q| < 1$, in this case we can completely compute the Tate module using the isomorphism $\overline{\mathbb{Q}_p}^\times/q^{\mathbb{Z}} \xrightarrow{\sim} E_q\left(\overline{\mathbb{Q}_p}\right)$. We have that $E_q[\ell^n] = \left\{[x] \in \overline{\mathbb{Q}_p}^\times/q^{\mathbb{Z}} \mid \left[x^{\ell^n}\right] = [1]\right\}$, that is we are looking for $x \in \overline{\mathbb{Q}_p}^\times$ such that $x^{\ell^n} \in q^{\mathbb{Z}}$. Choose an ℓ^n-th root of q, which for ease of notation we denote by q_{ℓ^n}, then any $x = \zeta_{\ell^n}^a q_{\ell^n}^b$ is a solution because $x^{\ell^n} = q^b \in q^{\mathbb{Z}}$, therefore we get

Corollary 5. *As a group,* $E_q[\ell^n] \cong \mathbb{Z}/\ell^n \times \mathbb{Z}/\ell^n$, *with basis given by* $\zeta_{\ell^n}, q_{\ell^n}$.

We now move to compute the Galois action. Recall that by definition G acts on ζ_{ℓ^n} via the cyclotomic trace, i.e. $g\zeta_{\ell^n} = \zeta_{\ell^n}^{\chi(g)}$. Now, as $q \in \mathbb{Q}_p$ is in the base field, it is Galois invariant, i.e. $gq = q$. Therefore, g sends q_{ℓ^n} to itself multiplied by a root of unity, i.e. $gq_{\ell^n} = \zeta_{\ell^n}^{c(g)} q_{\ell^n}$ for some $c(g) \in \mathbb{Z}/\ell^n$ (which depends on q), analogously to the cyclotomic character, thus we get

Corollary 6. *The* G *action on the basis of* $E_q[\ell^n] \cong \mathbb{Z}/\ell^n \times \mathbb{Z}/\ell^n$ *is given by the matrix*

$$\begin{pmatrix} \chi(g) & c(g) \\ 0 & 1 \end{pmatrix}$$

so, as a Galois representation $E_q[\ell^n]$ *is an extension of* $\mathbb{Z}/\ell^n$ *by* $\mathbb{Z}/\ell^n(1)$ *classified by* c.

References

[Li] Chao Li. *Mumford curves*. URL: http://www.math.columbia.edu/~chaoli/docs/MumfordCurves.html.

[Mie] Yoichi Mieda. *Introduction to p-adic uniformization of Shimura curves*. URL: https://www.ms.u-tokyo.ac.jp/~mieda/pdf/p-adic-uniformization.pdf.

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

[Sil11] Joseph H Silverman. *Advanced topics in the arithmetic of elliptic curves*. Springer, 2011.