Torsion of elliptic curves over local fields

1 Introduction

The goal of this text is to give two rather similar proofs of the fact that for any elliptic curve over a locally compact local field the torsion subgroup is finite. This result has already been obtained in the case when the field of definition is of characteristics 0 as is done for example in [1] in the more general case of abelian varieties. The idea of both proofs is quite simple: we find a pro-$p$-subgroup of the group of points, prove that its torsion is finite and prove that it is of finite index.

2 Notation

$K$ always denotes a local field whose residue field $k$ is finite of characteristics $p$. The discrete valuation on this field is denoted $v$, the ring of integers $R = \{ x \in K | v(x) \geq 0 \}$, the group of units $R^* = \{ x \in K | v(x) = 0 \}$, the maximal ideal $m = \{ x \in K | v(x) > 0 \}$. $E$ is an elliptic curve over $K$ with discriminant $\Delta$ and $j$-invariant $j$, its group of points over $K$ is denoted as $E(K)$. If $G$ is an abelian group, its torsion is denoted as $\text{Tor}(G)$, its $p$-primary torsion is denoted as $\text{Tor}_p(G)$.

3 Specialization of elliptic curves

The material of this section can be completely retold in the language of Néron models but for the sake of simplicity we use instead minimal Weierstrass equations of elliptic curves. In this section we follow [3].

Let $E$ be an elliptic curve given by the equation

$$y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6.$$

If we make the change of coordinates $(x, y) \mapsto (u^{-2} x, u^{-3} y)$, all $a_i$ become $u^i a_i$, so by choosing $u$ such that $v(u)$ is big enough we can obtain an equation whose coefficients lie in $R$.

**Definition 3.1.** A Weierstrass equation of $E$ is called minimal if for all $i a_i \in R$ and $v(\Delta)$ is minimal among all other such Weierstrass equations of this curve.

**Proposition 3.2.** For each elliptic curve $E$ a minimal Weierstrass equation exists and is unique up to a change of coordinates

$$x = u^2 x' + r$$

$$y = u^3 y' + u^2 s x + t,$$

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


Let us now assume that the equation of the curve is minimal. Then we can reduce the coefficients of the curve modulo \( m \) and obtain a cubic curve \( \tilde{E} \) over \( k \). This gives the specialization map \( E(K) \to \tilde{E}(k) \): \( P \mapsto \tilde{P} \).

There are three cases:

1. \( \tilde{E} \) is an elliptic curve. Then \( E \) is said to have good reduction.

2. \( \tilde{E} \) is a curve with singularity. Then \( E \) is said to have bad reduction.
   - If \( \tilde{E} \) is a nodal curve then the reduction is said to be multiplicative.
   - If \( \tilde{E} \) is a cuspidal curve then the reduction is said to be additive.

It’s not difficult to notice that in all three cases \( \tilde{E}_{ns}(k) \) has the structure of an abelian group with zero point \( \tilde{O} \). In the following discussion we denote \( E_0(K) = \{ P \in E(K) | \tilde{P} \in \tilde{E}_{ns}(k) \} \), \( E_1(K) = \{ P \in E(K) | \tilde{P} = \tilde{O} \} \). Both \( E_0(K) \) and \( E_1(K) \) are subgroups of \( E(K) \).

**Proposition 3.3.** There is an exact sequence of abelian groups:

\[
0 \to E_1(K) \to E_0(K) \to \tilde{E}_{ns}(k) \to 0,
\]

where the second map is the specialization map.

The use of this exact sequence is the crucial point in both proofs of the finiteness of torsion given here.

The group \( E_1(K) \) can be characterized in a different way.

**Proposition 3.4.** Let \( \hat{E}/R \) be the formal group of \( E \), \( \hat{E}(m) \) – the group associated to \( \hat{E} \). Then

\[
E_1(K) \cong \hat{E}(m).
\]

## 4 Torsion in \( E_0(K) \)

Both proofs of the main result start by the proof that \( Tor(E_0(K)) \) is finite but let us first examine the torsion in \( E_1(K) \).

**Proposition 4.1.** Let \( n \in \mathbb{Z} \) be coprime to \( \text{char } k = p \). Then there is no non-trivial \( n \)-torsion in \( E_1(K) \).

**Proof.** Let \( \hat{E} \) be a formal group law associated to \( E \) given by a series with coefficients in \( R \) and let us denote by \([n]\) the multiplication by \( n \). Then \([n]x = nx + x^2 f(x)\) where \( f(x) \) is some series over \( R \). \( n \) is coprime to \( p \), \( n \in R^* \), hence there exists a unique series \([n^{-1}]x\) inverse to \([n]x\) relative to the composition. It means that the multiplication by \( n \) is an isomorphism in \( \hat{E}(m) = E_1(K) \). We obtain that the only \( n \)-torsion element in \( E_1(K) \) is zero. \( \square \)

However, there might exist non-trivial \( p \)-primary torsion. In the following proposition we prove that it is finite. Hence, we will obtain that \( Tor(E_1(K)) \) is finite.
Proposition 4.2. The group $\text{Tor}_p(E_1(K))$ is finite.

Proof. If $\hat{E} \in R[[x,y]]$ is a formal group law let us denote $\hat{E}_i$ its reduction modulo the ideal $(x,y)^i$. Then $\hat{E}_i$ turns the set $\mathfrak{m}/\mathfrak{m}^i$ into the abelian group $\hat{E}_i(\mathfrak{m})$ and $\hat{E}(\mathfrak{m}) \cong \lim_i \hat{E}_i(\mathfrak{m})$. Hence $E_0(K)$ is a pro-$p$-group.

Suppose that $\text{Tor}_p(E_1(K))$ is infinite. As for each $n$ the $p^n$-torsion is finite there must exist a non-zero infinitely $p$-divisible element $x$. Indeed, for each $x \in E_1(K)$ let us denote $A_x := \{ y \in E_1(K) | \exists n \in \mathbb{N} p^n y = x \}$. Choose non-zero element $x_1$ in $p$-torsion such that $A_{x_1}$ is infinite. Then among its preimages by the multiplication by $p$ map choose $x_2$ such that $A_{x_2}$ is infinite. Continuing in this way we obtain an infinite sequence of non-zero elements $\{x_1, x_2, \ldots\}$ such that $px_n = x_{n-1}$. As there is no infinitely $p$-divisible elements in finite groups, $x$ must map to zero in each $\hat{E}_n(\mathfrak{m})$. Hence it is zero. Contradiction. \qed

From the results obtained above we get

Proposition 4.3. The group $\text{Tor}(E_0(K))$ is finite.

Proof. From the exact sequence (3.1) we see that $[E_0(K) : E_1(K)] < \infty$ hence $[\text{Tor}(E_0(K)) : \text{Tor}(E_1(K))] < \infty$. \qed

Remark 4.4. In fact there is a more direct way to prove that $E_0(K)$ is a profinite group (of course, not necessarily a pro-$p$-group). Let us take a minimal Weierstrass equation of $E$ and reduce its coefficients modulo $\mathfrak{m}^i$. We will denote the resulting curve $E'$ and its subgroup of $R/\mathfrak{m}^i$-points which map to $\hat{E}_i^n(k)$ after reducing modulo $\mathfrak{m}$ by $\hat{E}_i^n(R/\mathfrak{m}^i)$. Then we have the following proposition:

Proposition 4.5. The natural map $E_0(K) \to \varprojlim \hat{E}_i^n(R/\mathfrak{m}^i)$ is an isomorphism of groups.

The proposition easily follows from the following analogue of Hensel lemma.

Lemma 4.6. Let $R$ be a a ring complete in $I$-adic topology and $f \in R[[x_1,\ldots,x_n]]$. Suppose there exist $\alpha = (\alpha_1,\ldots,\alpha_n) \in R^n$ such that $f(\alpha_1,\ldots,\alpha_n) \in I$ and $I + (\frac{\partial f}{\partial x_1}(\alpha),\ldots,\frac{\partial f}{\partial x_n}(\alpha)) = (1)$. Then there exist $\beta = (\beta_1,\ldots,\beta_n) \in R^n$ such that $\beta_i \equiv \alpha_i \pmod I$ and $f(\beta_1,\ldots,\beta_n) = 0$. (Of course, such $\beta$ is not unique when $n > 1$).

Proof. The proof goes by induction. Suppose we have found $\beta^{(m)} = (\beta_1^{(m)},\ldots,\beta_n^{(m)})$ such that $\beta_1^{(m)} \equiv \alpha_1 \pmod I$ and $f(\beta_1^{(m)},\ldots,\beta_n^{(m)}) \in I^m$. Then we have to find $\beta^{(m+1)} \equiv \beta^{(m)} \pmod {I^{m-1}}$ with the same properties. We will make use of the following identity

$$f(\beta_1^{(m)} + \gamma_1,\ldots,\beta_n^{(m)} + \gamma_n) = f(\beta_1^{(m)},\ldots,\beta_n^{(m)}) + \sum_{i=1}^n \frac{\partial f}{\partial x_i}(\beta^{(m)})\gamma_i + \varepsilon,$$

where $\gamma_i \in I^m$, $\varepsilon \in I^{m+1}$. We need to choose $\gamma$ such that
\[ \sum_{i=1}^{n} \frac{\partial f}{\partial x_i}(\beta^{(m)})_{\gamma_i} \equiv -f(\beta_1^{(m)}, \ldots, \beta_n^{(m)}) \mod I^{m+1}. \]

This is always possible since
\[ I^m \left( \frac{\partial f}{\partial x_1}(\beta^{(m)}), \ldots, \frac{\partial f}{\partial x_n}(\beta^{(m)}) \right) + I^{m+1} = I^m. \]

\[ \square \]

5 Analytic topology on elliptic curves

In this section we will introduce a topology on the space of $K$-points of projective varieties over a topological field $K$ different from Zariski topology. We will make it in three steps:

1. The topology on $\mathbb{A}^n$ is just the product topology.

2. $\mathbb{P}^n$ is got by gluing $n+1$ copies of $\mathbb{A}^n$. As the transition maps are biregular we get the topology on $\mathbb{P}^n$.

3. The topology on any projective variety is the induced topology.

Let now $K$ be a locally compact field. Then we have the following proposition:

**Proposition 5.1.** Any projective variety over $K$ is compact in the analytic topology.

**Proof.** It is enough to show that $\mathbb{P}^n$ is compact. But it is the union of $n+1$ sets $A_i = \{ [x_0 : \ldots : 1 : \ldots : x_n] \in \mathbb{P}^n | v(x_j) \geq 0 \}$ which are compact as they are homeomorphic to $B_0(1)^n$ where $B_0(1)$ is a unit disk of radius 1. \[ \square \]

In particular, elliptic curves are compact in analytic topology.

Now we are ready to give the first proof of the main theorem.

**Theorem 5.2.** The group $\text{Tor}(E(K))$ is finite.

**Proof.** We have already proved in the previous section that $\text{Tor}(E_0(K))$ is finite. So it is enough to show that the index of $E_0(K)$ in $E(K)$ is finite. As the specialization map is continuous for the analytic topology and $\tilde{E}_{ns}(k)$ is open, so is $E_0(K)$ (it is also closed). But an open subgroup of a compact group has finite index. \[ \square \]

**Remark 5.3.** In fact $[E(K) : E_0(K)]$ is finite for an elliptic curve over any local field, not necessarily locally compact. The proof is due to Kodaira-Néron and relies on the classification of special fibers of Néron models.
6 \ p\text{-}adic uniformization

In this section, following [4], we construct an analytic homomorphism from \(K^*\) to an elliptic curve.

Let us fix \(t \in m\) and define the following two series:

\[
x(w) := \sum_{m=-\infty}^{\infty} \frac{t^m w}{(1 - t^m w)^2} - 2 \sum_{m=1}^{\infty} \frac{t^m}{(1 - t^m)^2}
\]

(6.1)

\[
y(w) := \sum_{m=-\infty}^{\infty} \frac{(t^m w)^2}{(1 - t^m w)^3} + \sum_{m=1}^{\infty} \frac{t^m}{(1 - t^m)^2}.
\]

(6.2)

It’s not hard to prove that both series converge absolutely for \(w \in K^*\) and uniformly on compact subsets. After some calculations one obtains the following formula:

\[
y^2 + xy = x^3 - b_2 x - b_3,
\]

(6.3)

where

\[
b_2 = 5 \sum_{n=1}^{\infty} \frac{n^3 t^n}{1 - t^n}
\]

(6.4)

\[
b_3 = \sum_{n=1}^{\infty} \left( \frac{7n^5 + 5n^3}{12} \right) \frac{t^n}{1 - t^n}.
\]

(6.5)

Let us call the elliptic curve defined by equation (6.3) \(E_t\). It is worth mentioning that its \(j\)-invariant equals

\[
j = t^{-1}(1 + 744t + 196884t^2 + ...)
\]

so the curve \(E_t\) always has bad reduction.

It would be natural to conjecture that the map \(\varphi: K^* \to E_t\) which sends \(w\) to \((x(w), y(w))\) is an analytic homomorphism. In fact this guess is true.

**Theorem 6.1** (Tate). The map \(\varphi: K^* \to E_t(K)\) is a surjective analytic homomorphism whose kernel is \(tZ\).

Now it’s not difficult to prove the main theorem in the case of Tate curves.

**Proposition 6.2.** The group \(\text{Tor}(E_t(K))\) is finite.

**Proof.** First we notice that the index of \(R^*\) in \(K^*/tZ\) is finite and is equal to \(v(t)\). So it’s enough to show that \(\text{Tor}(R^*)\) is finite. The \(n\)-torsion for \(n\) coprime to \(p\) is finite by Hensel lemma and \(p\)-primary torsion is finite by the following reason. Firstly, when the characteristics is \(p\) there is no non-trivial \(p\)-torsion and hence no \(p\)-primary torsion. When the characteristics is zero, \(K\) is a finite extension of \(\mathbb{Q}_p\). By examining the polynomial \(x^{p^{n+1}} - 1\) we see that it’s irreducible over \(\mathbb{Q}_p\) by Eisenstein criterion (we need to replace \(x\) by \(t + 1\)). Hence \([\mathbb{Q}_p(t^{p^{n+1}}) : \mathbb{Q}_p] = p^n(p - 1)\), so if \([K : \mathbb{Q}_p] < p^n(p - 1)\), \(K\) contains no primitive root of degree \(p^{n+1}\). \(\square\)
Above we have proved the theorem in two cases: of curves with good reduction and of Tate curves. The following lemma finishes the proof:

**Lemma 6.3.** Let $E$ be an elliptic curve over $K$. Then there is a finite extension $L/K$ such that $E/L$ is either a curve with good reduction or a Tate curve.

**Proof.** Suppose $v(j(E)) \geq 0$. By [3],Ch.VII,Prop.5.5 it follows that in this case the curve has potentially good reduction, i.e. has good reduction after a finite extension of scalars. Now suppose that $v(j(E)) < 0$. In [2],Ch.V,Lemma 5.1 it is proved that in this case $E$ is isomorphic to the unique Tate curve over $\bar{K}$ and hence over a finite extension of $K$.

**References**


