On the structure of elliptic curves over finite extensions of $\mathbb{Q}_p$ with additive reduction

Michiel Kosters and René Pannekoek

July 9, 2018

Abstract

Let $p$ be a prime and let $K$ be a finite extension of $\mathbb{Q}_p$. Let $E/K$ be an elliptic curve with additive reduction. In this paper, we study the topological group structure of the set of points of good reduction of $E(K)$. In particular, if $K/\mathbb{Q}_p$ is unramified, we show how one can read off the topological group structure from the Weierstrass coefficients defining $E$.

1 Introduction

In this article, we fix a prime $p$. Let $K/\mathbb{Q}_p$ be a finite extension. Let $\mathcal{O}_K$ be the ring of integers of $K$ with maximal ideal $m_K$ and residue field $k$. Let $E/K$ be an elliptic curve with additive reduction, given by a Weierstrass equation over $\mathcal{O}_K$ of the form

$$Y^2 + a_1 XY + a_3 Y = X^3 + a_2 X^2 + a_4 X + a_6,$$

with $a_i \in m_K$ for each $i$.

We denote by $E_0(K) \subset E(K)$ the subgroup of points that reduce to a non-singular point of the reduction curve defined over $k$.

The purpose of this paper is to investigate the structure of $E_0(K)$ as a topological group and as a $\mathbb{Z}_p$-module. We first show that $p$-adic topology on $E_0(K)$ from the embedding into $\mathbb{P}^2(K)$ agrees with the topology from the $\mathbb{Z}_p$-module structure (Proposition 6 and Proposition 5). Our main theorem is the following, where $N_{k/\mathbb{F}_p} : k \to \mathbb{F}_p$ is the norm map.

**Theorem 1.** Assume that $K/\mathbb{Q}_p$ is unramified of degree $n$ with ring of integers $\mathcal{O}_K$, maximal ideal $m_K$ and residue field $k$. Let $E/K$ be an elliptic curve given by a Weierstrass equation over $\mathcal{O}_K$ of the form

$$Y^2 + a_1 XY + a_3 Y = X^3 + a_2 X^2 + a_4 X + a_6,$$

with $a_i \in m_K = p\mathcal{O}_K$ for each $i$. Then one has $E_0(K) \cong \mathbb{Z}_p \mathbb{Z}_p^n$, except in the following four cases:
(i) \( p = 2 \) and the equation \( \frac{a_3}{2}x^3 + \frac{a_1}{2}x - 1 = 0 \) has a solution in \( k \); 
(ii) \( p = 3 \) and \( N_{k/F_p}(8a_2/3) = 1 \); 
(iii) \( p = 5 \) and \( N_{k/F_p}(3a_4/5) = 1 \); 
(iv) \( p = 7 \) and \( N_{k/F_p}(4a_6/7) = 1 \).

In case (i), one \( E_0(Q_2) \cong \mathbb{Z}_2 \times (\mathbb{Z}/2\mathbb{Z})^b \) where \( 2^b \) is the number of solutions to \( \frac{a_3}{2}X^4 + \frac{a_1}{2}X^2 - X = 0 \) in \( k \). In the cases (ii)-(iv), one has \( E_0(Q_p) \cong \mathbb{Z}_p \mathbb{Z}_p^n \times \mathbb{Z}/p\mathbb{Z} \).

The above theorem gives the following result for \( K = Q_p \).

**Corollary 2.** Let \( E/Q_p \) be an elliptic curve given by a Weierstrass equation over \( \mathbb{Z}_p \)

\[
Y^2 + a_1 XY + a_3 Y = X^3 + a_2 X^2 + a_4 X + a_6,
\]

with \( a_i \in p\mathbb{Z}_p \) for each \( i \). One has \( E_0(Q_p) \cong \mathbb{Z}_p \mathbb{Z}_p \) unless one is in one of the four special cases:

(i) \( p = 2 \) and \( a_1 + a_3 \equiv 2 \pmod{4} \);
(ii) \( p = 3 \) and \( a_2 \equiv 6 \pmod{9} \);
(iii) \( p = 5 \) and \( a_4 \equiv 10 \pmod{25} \);
(iv) \( p = 7 \) and \( a_6 \equiv 14 \pmod{49} \).

In all special cases one has \( E_0(Q_p) \cong \mathbb{Z}_p \mathbb{Z}_p^n \times \mathbb{Z}/p\mathbb{Z} \).

Note that any curve with additive reduction can be written in the form of Theorem 1 (Lemma 9). The case \( p > 7 \) of Theorem 1 was also mentioned in [3, Lemma 1].

We obtain the following result when \( K/Q_p \) is ramified.

**Theorem 3.** Assume that \( K/Q_p \) is of degree \( n \) and that the ramification index is \( e \). If \( 6e < p - 1 \), then one has \( E_0(K) \cong \mathbb{Z}_p \mathbb{Z}_p^n \).

We will briefly discuss some of the exceptional cases for ramified extensions, but we do not obtain a completely satisfying answer.

We will say a few words about the idea of the proofs. Let \( K/Q_p \) be a finite extension. It is a standard fact from the theory of elliptic curves over local fields [2, VII.6.3] that \( E_0(K) \) admits a canonical filtration

\[
E_0(K) \supset E_1(K) \supset E_2(K) \supset E_3(K) \supset \ldots,
\]

where for each \( i \geq 1 \) the quotient \( E_i(K)/E_{i+1}(K) \) is isomorphic to \( k \). The quotient \( E_0(K)/E_1(K) \) is also isomorphic to \( k \) by the fact that \( E \) has additive reduction. The groups \( E_i(K) \) for \( i \geq 1 \) can be seen as formal groups, and since our curve has additive reduction, \( E_0(K) \) can also be seen as a formal group (Proposition 12). For large enough
the theory of formal groups gives an isomorphism \( j : E_j(K) \rightarrow \mathfrak{m}_K^j \). The idea is then to explicitly use the exact sequence \( 0 \rightarrow E_j(K) \rightarrow E_{j-1}(K) \rightarrow k \rightarrow 0 \) to compute the structure of \( E_{j-1}(K) \). We keep doing this, until we (hopefully) get the structure of \( E_0(K) \). In the case that \( K \) is unramified over \( \mathbb{Q}_p \), the computations become easier, since one already has \( E_1(K) \cong \mathfrak{m}_K \) (Proposition 10), and we have to study only one exact sequence to obtain the structure of \( E_0(K) \).

This paper is a generalization of [1] and hence contains some overlap.

2 Preliminaries

2.1 Weierstrass curves

All proofs of facts recalled in this section can be found in [2, IV and VII].

Let \( p \) be a prime. Let \( K \) be a finite field extension of \( \mathbb{Q}_p \) of degree \( n \) and ramification degree \( e \). Let \( v_K : K \rightarrow \mathbb{Z} \cup \{\infty\} \) be its normalized valuation. Let \( \mathcal{O}_K \) be the ring of integers, \( \mathfrak{m}_K \) its maximal ideal and \( k \) its residue field. By a Weierstrass curve over \( \mathcal{O}_K \) we mean a projective curve \( E \subset \mathbb{P}^2_{\mathcal{O}_K} \) defined by a Weierstrass equation

\[
Y^2 + a_1 XY + a_3 Y = X^3 + a_2 X^2 + a_4 X + a_6,
\]

such that the generic fiber \( E_K \) is an elliptic curve with \((0 : 1 : 0)\) as the origin. The coefficients \( a_i \in \mathcal{O}_K \) are uniquely determined by \( E \).

The set \( \mathbb{P}^2(K) \) has the quotient topology from \( K^3 \) where \( K \) has the \( p \)-adic topology. This induces a topology on \( E(K) \) and makes \( E(K) \) into a topological group. We call this topology the standard topology.

We will say that a Weierstrass curve \( E/\mathcal{O}_K \) has good reduction when the special fiber \( \tilde{E} = E_k \) is smooth, multiplicative reduction when \( \tilde{E} \) is nodal (i.e. there are two distinct tangent directions to the singular point), and additive reduction when \( \tilde{E} \) is cuspidal (i.e. one tangent direction to the singular point).

We have \( E(K) = E(\mathcal{O}_K) \) since \( E \) is projective. Therefore, we have a reduction map \( E(K) \rightarrow \tilde{E}(k) \) given by restricting an element of \( E(\mathcal{O}_K) \) to the special fiber. Let \( \tilde{E}_{sm}(k) \) be the complement of the singular points in the special fiber \( \tilde{E}(k) \), which is a group. We denote the preimage of \( \tilde{E}_{sm}(k) \) under the reduction map by \( E_0(k) \). The standard topology makes \( E_0(K) \) into a topological group. By \( E_1(K) \subset E_0(K) \) we denote the kernel of reduction, i.e. the points that map to the identity \( \infty \) of \( \tilde{E}(k) \). A more explicit definition of \( E_1(K) \) is

\[
E_1(K) = \{(x, y) \in E(K) : v_K(x) \leq -2, v_K(y) \leq -3\} \cup \{\infty\}.
\]

More generally, one defines subgroups \( E_n(K) \subset E_0(K) \) as follows [2, ex. 7.4]:

\[
E_n(K) = \{(x, y) \in E(K) : v_K(x) \leq -2n, v_K(y) \leq -3n\} \cup \{\infty\}.
\]
We thus have an infinite filtration on the subgroup $E_1(K)$:

$$E_1(K) \supset E_2(K) \supset E_3(K) \supset \cdots$$  \hspace{1cm} (3)

This gives us a filtration of open neighborhoods around $\infty$ of $E_0(K)$.

We have an exact sequence \cite{2} VII.2.1:

$$0 \to E_1(K) \to E_0(K) \to \tilde{E}_{sm}(k) \to 0. \hspace{1cm} (4)$$

If $\tilde{E}$ is smooth, $\tilde{E} = \tilde{E}_{sm}(k)$ is an elliptic curve. If $\tilde{E}$ is cuspidal, one has $\tilde{E}_{sm}(k) \cong k^*$ or $\tilde{E}_{sm}(k) \cong \{c \in I : N_{l/k}(c) = 1\}$ where $l/k$ is of degree 2. We call this multiplicative reduction. If $E_k$ is nodal, one has $\tilde{E}_{sm}(k) \cong k^+$. We call this additive reduction. Assume that $\tilde{E}$ has additive reduction. If $(0,0)$ is the node, and the tangent line is given by $Y = 0$, that is, the equation for the reduction is of the form $Y^2 = X^3$, then one has an isomorphism $\tilde{E}_{sm}(k) \to k^+$ is given by $(x,y) \mapsto -x/y$. See \cite{2} III.2.5. In the case that the curve is minimal and of additive reduction, the quotient $E(K)/E_1(K)$ has order at most 4 \cite{2} VII.6.1.

We denote the formal group corresponding to $E$ by $\hat{E}$ \cite{2} IV.1–2. This is a one-dimensional formal group over $O_K$. Giving the data of this formal group is the same as giving a power series $F = F_{\hat{E}}$ in $O_K[[X,Y]]$, called the formal group law. It satisfies

$$F(X, Y) = X + Y + \text{(terms of degree } \geq 2)$$

and

$$F(F(X, Y), Z)) = F(X, F(Y, Z)).$$

For $E$ as in \cite{1}, the first few terms of $F$ are given by:

$$F(X, Y) = X + Y - a_1XY - a_2(X^2Y + XY^2) - 2a_3(X^3Y + XY^3) + (a_1a_2 - 3a_3)X^2Y^2 - (2a_1a_3 + 2a_4)(X^4Y + XY^4) - (a_1a_3 - a_2^2 + 4a_4)(X^3Y^2 + X^2Y^3) + \ldots.$$  

In fact, $\hat{E}$ is a $\mathbb{Z}_p$-module (see \cite{2} ex. 4.3).

Treating the Weierstrass coefficients $a_i$ as unknowns, we may consider $F$ as an element of $\mathbb{Z}[a_1, a_2, a_3, a_4, a_6][[X, Y]]$, called the generic formal group law. If we make $\mathbb{Z}[a_1, a_2, a_3, a_4, a_6]$ into a weighted ring with weight function $wt$, such that $wt(a_i) = i$ for each $i$, then the coefficients of $F$ in degree $n$ are homogeneous of weight $n-1$ \cite{2} IV.1.1. For each $n \in \mathbb{Z}_{\geq 2}$, we define power series $[n]$ in $O_K[[T]]$ by $[2](T) = F(T, T)$ and $[n](T) = F([n-1](T), T)$ for $n \geq 3$. Here also, we may consider each $[n]$ either as a power series in $O_K[[T]]$ or as a power series in $\mathbb{Z}[a_1, a_2, a_3, a_4, a_6][[T]]$ called the generic multiplication by $n$ law. We have:

**Lemma 4.** Let $[p] = \sum b_i T^i \in \mathbb{Z}[a_1, a_2, a_3, a_4, a_6][[T]]$ be the generic formal multiplication by $p$ law. Then:
1. $p \mid b_i$ for all $i$ not divisible by $p$;
2. $\text{wt}(b_i) = i - 1$, considering $\mathbb{Z}[a_1, a_2, a_3, a_4, a_6]$ as a weighted ring as above.

**Proof.** (1) is proved in [2, IV.4.4]. (2) follows from [2, IV.1.1] or what was said above.

The series $F(u, v)$ converges to an element of $m_K$ for all $u, v \in m_K$. To $E$ one associates the group $\hat{E}(m_K)$, the $m_K$-valued points of $E$, which as a set is just $m_K$, and whose group operation $+$ is given by $u + v = F(u, v)$ for all $u, v \in \hat{E}(m_K)$. The identity element of $\hat{E}(m_K)$ is $0 \in m_K$. If $i \geq 1$ is an integer, then by $\hat{E}(m_K^i)$ we denote the subset of $\hat{E}(m_K)$ corresponding to the subset $m_K^i \subseteq m_K$, where $m_K^i$ is the $i$th power of the ideal $m_K$ of $O_K$.

The subsets $\hat{E}(m_K^i)$ are subgroups of $\hat{E}(m_K)$, and we have an infinite filtration of $\hat{E}(m_K)$:

$$\hat{E}(m_K) \supset \hat{E}(m_K^2) \supset \hat{E}(m_K^3) \supset \cdots .$$

(5)

One has $\hat{E}(m_K^i)/\hat{E}(m_K^{i+1}) \cong m_K^i/m_K^{i+1} \cong k^+$. For $i > e/(p - 1)$ one has $\hat{E}(m_K^i) \cong \mathbb{Z}_p m_K^i$ by a ‘logarithm’ map, and the following diagram commutes ([2, IV.6.4]):

$$\begin{array}{ccc}
\hat{E}(m_K^i) & \cong & \hat{E}(m_K^{i+1}) \\
\downarrow \sim & & \downarrow \sim \\
m_K^{i+1} & \rightarrow & m_K^i.
\end{array}$$

We make $\hat{E}(m_K)$ into a topological group by using the above filtration as a fundamental system of neighborhoods around 0. This means that a subset $U$ of $\hat{E}(m_K)$ is open if and only if for all $x \in U$ there is an $m \in \mathbb{Z}_{\geq 1}$ such that $x + \hat{E}(m_K^m) \subseteq U$. This is the same as the topology coming from the identification $\hat{E}(m_K) = m_K$ of sets and then using the $p$-adic topology from $K$ on $m_K$. We call this the standard topology.

**Proposition 5.** The map

$$\psi_K : E_1(K) \xrightarrow{\sim} \hat{E}(m_K)$$

$$(x, y) \mapsto -x/y$$

$$0 \mapsto 0$$

is an isomorphism of topological groups. Moreover, $\psi_K$ respects the filtrations (2) and (5), i.e. it identifies the subgroups $E_i(K)$ defined with $\hat{E}(m_K^i)$ for $i \in \mathbb{Z}_{\geq 1}$.

**Proof.** See the proof of [2, VII.2.2]: the maps are homeomorphisms. 

Given a finite field extension $L \supseteq K$, we have a natural commutative diagram

$$\begin{array}{ccc}
E_1(K) & \xrightarrow{\psi_K} & \hat{E}(m_K) \\
\downarrow \text{incl} & & \downarrow \text{incl} \\
E_1(L) & \xrightarrow{\psi_L} & \hat{E}_{O_L}(m_L)
\end{array}$$
Here $E_{O_L}(m_L)$ is the set of $m_L$-valued points of the formal group of $E_{O_L}$, the base-change of $E$ to $\text{Spec}(O_L)$.

Let $G$ be a finitely generated $\mathbb{Z}_p$-module. We make $G$ into a topological group by using the filtration $\{p^i G : i \in \mathbb{Z}_{\geq 0}\}$ of neighborhoods around 0. We call this the $\mathbb{Z}_p$-topology.

**Proposition 6.** The group $E_0(K)$ is a finitely generated $\mathbb{Z}_p$-module. Furthermore, the $\mathbb{Z}_p$-module topology and the standard topology on $E_0(K)$ coincide.

**Proof.** We use Proposition [5]. Note that $E_0(K)/E_1(K)$ is finite. One has $E_i(K)/E_{i+1}(K) \cong k^+$ for $i \geq 1$, and for large enough $i$ one has $E_i(K) \cong \mathbb{Z}_p \cdot m_i$. Note that $m_i$ is finitely generated and hence $E_i(K)$ is finitely generated. This shows that $E_0(K)$ is finitely generated.

For large enough $i$ one has $pE_i(K) \cong pm_i \cong m_i \cong E_{i+1}(K)$. Hence the filtrations of neighborhoods give the same topology.

\[\square\]

### 2.2 Commutative algebra

**Lemma 7.** Let $a, n \in \mathbb{Z}_{\geq 0}$. Let

$$0 \to \mathbb{Z}_p^n \xrightarrow{i} G \xrightarrow{\pi} H \to 0$$

be an exact sequence of $\mathbb{Z}_p$-modules where $H$ is finitely generated and $p^n$-torsion. Let $\tau : \mathbb{Z}_p^n \to \mathbb{Z}_p^n/p^n \mathbb{Z}_p^n$ be the natural quotient map. Define

$$g : H \to \mathbb{Z}_p^n/p^n \mathbb{Z}_p^n, \quad \pi(x) \mapsto \tau(p^n x).$$

Then $g$ is a well-defined morphism of $\mathbb{Z}_p$-modules and one has $G \cong \mathbb{Z}_p^n \oplus \text{ker}(g)$. Furthermore, if $\text{ker}(g) = 0$, one can identify $G$ with $1/p^n(\pi^{-1}\text{im}(g)) \supseteq \mathbb{Z}_p^n$ inside $\mathbb{Q}_p^n$.

**Proof.** Consider the morphism $h : G \to \mathbb{Z}_p^n/p^n \mathbb{Z}_p^n, \quad x \mapsto \tau(p^n x)$. Note that $h|_H = 0$, so this morphism induces the map $g$ with $h = g \circ \pi$. By the structure theorem for finitely generated $\mathbb{Z}_p$-modules we have $G \cong \mathbb{Z}_p^n \oplus G[p^n]$. We claim $G[p^n] + \mathbb{Z}_p^n = \text{ker}(h)$. Note that $G[p^n] + \mathbb{Z}_p^n \subseteq \text{ker}(h)$. Let $x \in \text{ker}(h)$. Then one has $p^n x \in p^n \mathbb{Z}_p^n$, equivalently $p^n (x - c) = 0$ for some $c \in \mathbb{Z}_p^n$. We conclude $x \in G[p^n] + \mathbb{Z}_p^n$. Since $\pi$ is surjective, and trivial on $\mathbb{Z}_p^n$, and injective on $G[p^n]$, the kernel of $g$ is isomorphic to $G[p^n]$.

Assume that $g$ is injective. One has $\tau^{-1}\text{im}(g) = p^n G$, and from this the final result follows easily.

\[\square\]

**Lemma 8.** Let $k$ be a finite field of characteristic $p$. Consider the additive polynomial

$$f = X - aX^p \in k[x] \quad \text{with} \quad a \in k^*.$$  

Then $f$ has all its roots in $k$ if and only if $a$ is a $(p-1)^{st}$ power, that is, if and only if $N_{k/F}(a) = a^{(p^k-1)/(p-1)} = 1$.

**Proof.** The roots in $k$ form a subgroup form a group isomorphic to $\mathbb{Z}/p\mathbb{Z}$. The polynomial $f$ has a non-trivial root in $k$ if and only if $1/a = X^{p-1}$ has a solution, that is, if and only if $a$ is a $(p-1)^{st}$ power.

\[\square\]
3 Weierstrass curves with additive reduction over $\mathcal{O}_K$

As in Section 2, let $K$ be a finite extension of $\mathbb{Q}_p$ of degree $n$. Let $\mathcal{O}_K$ be the ring of integers of $K$, with maximal ideal $\mathfrak{m}_K$ and residue field $k$ and ramification degree $e = e(K/\mathbb{Q}_p)$.

In this section, we study Weierstrass curves over $\mathcal{O}_K$ with additive reduction.

**Lemma 9.** Let $E/\mathcal{O}_K$ be a Weierstrass curve with additive reduction. Then $E$ is $\mathcal{O}_K$-isomorphic to a Weierstrass curve of the form

$$Y^2 + a_1 XY + a_3 Y = X^3 + a_2 X^2 + a_4 X + a_6,$$

where all $a_i$ lie in $\mathfrak{m}_K$.

**Proof.** We construct an automorphism $\alpha \in \text{PGL}_3(\mathcal{O}_K)$ that maps $E$ to a Weierstrass curve of the desired form. Consider a translation $\alpha_1 \in \text{PGL}_3(\mathcal{O}_K)$ moving the singular point of the special fiber $E_k$ to $(0 : 0 : 1)$. The image $E_1 = \alpha_1(E)$ is a Weierstrass curve with coefficients satisfying $a_3, a_4, a_6$ in $\mathfrak{m}_K$. There exists a second automorphism $\alpha_2 \in \text{PGL}_3(\mathcal{O}_K)$, of the form $X' = X, Y' = Y + cX$, such that in the special fiber of $\alpha_2(E_1)$ the unique tangent at $(0 : 0 : 1)$ is given by $Y' = 0$. The Weierstrass curve $E_2 = \alpha_2(E_1)$ now has all its coefficients $a_1, a_2, a_3, a_4, a_6$ in $\mathfrak{m}_K$. One may thus take $\alpha = \alpha_2 \circ \alpha_1$. \hfill \Box

From now on we assume that $E/\mathcal{O}_K$ is a Weierstrass curve given by (1), and we suppose that the $a_i$ are contained in $\mathfrak{m}_K$. In particular, $E$ has additive reduction.

3.1 $E_i(K), i > 0$

**Proposition 10.** Let $E/\mathcal{O}_K$ be a Weierstrass curve given by (1), and assume that the $a_i$ are contained in $\mathfrak{m}_K$. For $i > e/(p - 1)$ or if $p = 2$ and $i \geq e/(p - 1)$, one has $E_i(K) \cong \mathbb{Z}_p \mathbb{Z}_p$ and $pE_i(K) = E_{i+e}(K)$.

**Proof.** One has $E_i(K) \cong \hat{E}(m_i^i)$ as we have seen before. If $i > e/(p - 1)$, the result we want to prove is precisely [2] IV.6.4).

Assume $p = 2$ and $i > e/(p - 1) - 1 = e - 1$. Note $i \geq 1$ and one has $i + 1 > e/(p - 1)$. We have the exact sequence

$$0 \to \hat{E}(m_{K}^{i+1}) \to \hat{E}(m_{K}^{i}) \to m_i^i/m_{K}^{i+1} \cong k \to 0.$$

One has $2\hat{E}(m_{K}^{i+1}) = \hat{E}(m_{K}^{i+1+e})$. Set $[2](T) = \sum_j b_j T^j$. By Lemma 7 we have an induced map

$$g : m_i^i/m_{K}^{i+1} \to \hat{E}(m_{K}^{i+1})/\hat{E}(m_{K}^{i+1+e})$$

$$a \pmod{m_{K}^{i+1}} \mapsto [2](a) = \sum_j b_j a^j \pmod{\hat{E}(m_{K}^{i+1+e})}.$$
We then use Lemma 4. If \( j > 1 \) and \( 2 \nmid j \), one has \( v(b_j) \geq e + 1 \) and hence \( v(b_ja^j) \geq v(b_j) + v(a) \geq e + i + 1 \). If \( j = 2j' \geq 2 \), then one has \( v(b_j) \geq 1 = p - 1 \) (here we require \( p = 2 \)) and \( v(b_ja^j) \geq 1 + 2i > e + i \). As \( b_0 = 2 \), the induced map is just \( g: a \mapsto 2a \), which is injective. The image of \( g \) is \( \hat{E}(m^{i+e}_K)/\hat{E}(m^{i+1+e}_K) \). We can identify \( \hat{E}(m^{i+e}_K) \) with \( 1/2m^{i+e}_K = m^e_K \). In other words, one has \( 2E_i(K) = E_{i+e}(K) \). □

### 3.2 \( E_0(K) \): general theory

If we let \( F \) denote the formal group law of \( E \), then the assumption on the \( a_i \) implies that \( F(u, v) \) converges to an element of \( \mathcal{O}_K \) for all \( u, v \in \mathcal{O}_K \). Hence \( F \) can be seen to induce a group structure on \( \mathcal{O}_K \), extending the group structure on \( \hat{E}(m^e_K) \). The same statement holds true when we replace \( K \) by a finite field extension \( L \).

**Definition 11.** Let \( E/\mathcal{O}_K \) be a Weierstrass curve given by (1), and assume that the \( a_i \) are contained in \( m_K \). For any finite field extension \( L \supseteq K \), we denote by \( \hat{E}(\mathcal{O}_L) \) the topological group obtained by endowing the space \( \mathcal{O}_L \) with the group structure induced by \( F \).

The group \( \hat{E}(\mathcal{O}_K) \) is a \( \mathbb{Z}_p \)-module, and comes with the \( \mathbb{Z}_p \)-module topology (equivalently, the \( p \)-adic topology from the set \( \mathcal{O}_K \)).

**Theorem 12.** Let \( E/\mathcal{O}_K \) be a Weierstrass curve given by (1), and assume that the \( a_i \) are contained in \( m_K \).

1. The map \( \Psi: E_0(K) \to \hat{E}(\mathcal{O}_K) \) that sends \( (x, y) \) to \( -x/y \) is an isomorphism of topological groups.
2. If \( 6e < p - 1 \), then one has \( E_0(K) \cong \mathbb{Z}_p \mathbb{Z}_p^n \).
3. One has the following commutative diagram, where \( E_0(K) \to \hat{E}_{\text{sm}}(k) \cong k^+ \) is the reduction map:

\[
\begin{array}{ccc}
E_0(K) & \xrightarrow{(x,y)\mapsto -x/y} & \mathcal{O}_K \\
\Psi: (x,y)\mapsto -x/y & \downarrow & \uparrow \\
\hat{E}(\mathcal{O}_K) & \xrightarrow{x\mapsto \bar{x}} & k^+ \\
\end{array}
\]

**Proof.** Let \( \pi \) be a uniformizer for \( \mathcal{O}_K \). Consider the field extension \( L = K(\rho) \) with \( \rho^6 = \pi \). Then define the Weierstrass curve \( D \) over \( \mathcal{O}_L \) by

\[
Y^2 + \alpha_1 XY + \alpha_3 Y = X^3 + \alpha_2 X^2 + \alpha_4 X + \alpha_6,
\]

8
where $\alpha_i = \alpha_i/\rho^i$. There is a birational map $\phi : E \times_{O_K} O_L \dashrightarrow D$, given by $\phi(X,Y) = (X/\rho^2, Y/\rho^3)$. The birational map $\phi$ induces an isomorphism on generic fibers, and hence a homeomorphism between $E(L)$ and $D(L)$. Using (2) and the fact that we have $(x, y) \in E_0(L)$ if and only if $v_L(x), v_L(y)$ are both not greater than zero, one sees that $\phi$ induces a bijection $E_0(L) \sim \rightarrow D_1(L)$, that all maps (a priori just of sets) in the following diagram are well-defined, and that the diagram commutes:

$$
\begin{array}{ccc}
E_0(K) & \xrightarrow{\text{incl}} & E_0(L) \\
\downarrow{\psi} & & \downarrow{\psi_L} \\
\tilde{E}(O_K) & \xrightarrow{\text{incl}} & \tilde{E}(O_L) \xrightarrow{\rho} \tilde{D}(m_L).
\end{array}
$$

Here the map $\Psi_L : E_0(L) \rightarrow \tilde{E}(O_L)$ is defined by $(x, y) \mapsto -x/y$, the rightmost lower horizontal arrow is multiplication by $\rho$, and the maps labeled incl are the obvious inclusions. Let $F_{\tilde{D}}$ be the formal group law of $D$. One calculates that

$$
\rho F_{\tilde{D}}(X, Y) = F_{\tilde{D}}(\rho X, \rho Y).
$$

Hence $\cdot \rho, \psi_L$ (Proposition 5) and $\phi$ are homeomorphisms of groups. It follows that the group morphism $\Psi_L$ is a homeomorphism of groups. Hence $\Psi$ must be a homeomorphism onto its image. The map $\Psi_L$ is Galois-invariant, and hence by Galois theory, it follows that $\Psi$ is surjective, and that it is in fact a homeomorphism.

Now assume $6e(K/Q_p) < p - 1$, so that $v_L(p) = 6v_K(p) = 6e(K/Q_p) < p - 1$. Now [2 IV.6.4(b)] implies that $E_1(K)$ is isomorphic to $m_K$, and $D_1(L)$ to $m_L$. Since $E$ has additive reduction, we have $\tilde{E}_{\text{sm}}(k) \cong k^+$. We have an exact sequence

$$
0 \rightarrow m_K \rightarrow E_0(K) \rightarrow k^+ \rightarrow 0.
$$

In the diagram above, the topological group $E_0(K)$ is mapped homomorphically into the torsion-free group $D_1(L)$, hence it is itself torsion-free. It follows that $E_0(K)$ is isomorphic to $Z_p^\alpha$. This proves the second part.

The commutativity of the diagram follows directly. 

\[ \square \]

### 3.3 $E_0(K)$: special cases

In the previous subsection, we have seen that $E_0(K) \cong Z_p^\alpha$ if $p - 1 > 6e$. We have $E_1(K) \cong Z_p^\alpha$ if $p - 1 > e$, or if $p = 2$ and $e = 1$ (Proposition 10). We will study what happens with $E_0(K)$ in the latter case, so assume $p - 1 > e$, or $p = 2$ and $e = 1$. We implicitly identify $E_1(K)$ with $\tilde{E}(m_K^\alpha)$. We have an exact sequence

$$
0 \rightarrow E_1(K) \rightarrow E_0(K) \rightarrow \tilde{E}_{\text{sm}}(k) \cong k^+ \rightarrow 0.
$$

To compute the torsion of $E_0(K)$, we apply Lemma 7. We consider the induced group morphism $k \rightarrow E_1(K)/pE_1(K) = E_1(K)/E_{1+e}(K)$ (Proposition 10). Theorem 12 allows
one to compute the map explicitly. Consider the power series \([p](T)\) corresponding to the curve. One obtains a map \(g = [p](T) : k \to \tilde{E}(m_K^1)/\tilde{E}(m_K^{1+e})\). In general, the torsion of \(E_0(K)\) will be isomorphic to \(\text{ker}(g)\). If \([p](T) = \sum b_i T^i\), one can show that only the terms \(pT + \sum_{j > 0} (p_j - 1)/6 \leq e b_{p_j} T^{pj}\) play a role (Lemma 4). We see that the map is just \([p]T = pT\) if \((p - 1)/6 > e\), hence the kernel of \(g\) is trivial, and we recover part of Theorem 12. Given a field \(K\), one can explicitly find conditions on the \(a_i\) which determine the kernel of \(g\) and hence the structure of \(E_0(K)\). As an example, we study the case where \(e = 1\).

3.3.1 \(e = 1\)

This is the case where \(K/Q_p\) is unramified. We have a map \(g : k \to \tilde{E}(m_K^1)/\tilde{E}(m_K^2) \cong k\). Since the latter isomorphism is very explicit, we do not need logarithm to understand it. The map \(g\) is given by a polynomial. For \(p > 7\), this is the identity map and there is no torsion.

For \(p = 3, 5, 7\) this polynomial is of the form \(T - aT^p\). If \(n = 1\), then \(E_0(K) \cong \mathbb{Z}_p \times \mathbb{Z}/p\mathbb{Z}\) if \(a = 1\) and \(\mathbb{Z}_p\) otherwise. If \(n > 1\), then Lemma 8 tells us that this equation has a non-trivial solution over \(k\) if and only if \(a\) is a \((p - 1)\)st power in \(k\). In that case, \(E_0(K)\) is isomorphic to \(\mathbb{Z}_p^m \times \mathbb{Z}/p\mathbb{Z}\), and otherwise it is \(\mathbb{Z}_p^m\).

If \(p = 2\), the polynomial is of the form \(T - aT^2 - bT^4\). Lemma 8 can be used to handle the case when \(n = 1, 2\), but otherwise it is more tricky to see what the kernel of this map is. It shows that \(E_0(K)\) is isomorphic to \(\mathbb{Z}_p^3 \times (\mathbb{Z}/2\mathbb{Z})^i\) with \(i \in \{0, 1, 2\}\). Here \(2^i\) is the number of solutions of \(T - aT^2 - bT^4 = 0\) in \(k\).

For \(p = 2, 3, 5, 7\) we explicitly compute the polynomial \(g = [p](T)/p \pmod{pO_K}\).

| \(p\) | \([p](T)\) | \(g\) |
|---|---|---|
| 2 | \(2T - a_1 T^2 - 2a_2 T^3 + (a_1 a_2 - 7a_3) T^4 + \ldots\) | \(T - a_1/2T^2 - a_3/2T^4\) |
| 3 | \(3T - 3a_1 T^2 + (a_1^2 - 8a_2) T^3 + (12a_1a_2 - 39a_3) T^4 + \ldots\) | \(T - 8a_2/3T^3\) |
| 5 | \(5T - 1248a_4 T^5 + \ldots\) | \(T - 3a_4/5T^5\) |
| 7 | \(7T - 6720a_4 T^5 - 352944a_4 T^7 + \ldots\) | \(T - 4a_6/7T^7\) |

In all the above cases, if there is no torsion in \(E_0(K)\), then the map \(g\) is surjective, and by Lemma 11 one has \(pE_0(K) = E_1(K)\) (one identifies \(E_0(K)\) with \(O_K\) after the isomorphism \(\tilde{E}(m_K^1) \cong m_K\)).
Proof of Theorem \[\text{and Corollary}\] Follows from the discussion above (and Lemma \[\text{8}\]).

We will now list some examples of elliptic curves over \(\mathbb{Q}_p\) with additive reduction, such that their points of good reduction contain \(p\)-torsion points. In particular, all curves and torsion points are defined over \(\mathbb{Q}\). We also have an example of a curve over \(\mathbb{Q}_2(\zeta_3)\) having full 2-torsion in \(\mathbb{Q}(\zeta_3)\).

**Example 13.** The elliptic curve

\[ E_2 : Y^2 + 2Y = X^3 - 2 \]

has additive reduction at 2, and its 2-torsion point \((1, -1)\) is of good reduction.

In fact, if one considers this curve over \(\mathbb{Q}_2(\zeta_3)\), the unramified extension of \(\mathbb{Q}_2\) of degree 2, then the 2 torsion contains 4 points of good reduction defined over \(\mathbb{Q}(\zeta_3)\):

\[ \{\infty, (-\zeta_3, -1), (\zeta_3, -1), (1, -1)\}. \]

**Example 14.** The elliptic curve

\[ E_3 : Y^2 = X^3 - 3X^2 + 3X \]

has additive reduction at 3, and its 3-torsion point \((1, 1)\) is of good reduction.

**Example 15.** The elliptic curve

\[ E_5 : Y^2 - 5Y = X^3 + 20X^2 - 15X \]

has additive reduction at 5, and its 5-torsion point \((1, -1)\) is of good reduction.

**Example 16.** The elliptic curve

\[ E_7 : Y^2 + 7XY - 28Y = X^3 + 7X - 35 \]

has additive reduction at 7, and its 7-torsion point \((2, 1)\) is of good reduction.

**Example 17.** Consider the curve \(E_8 : Y^2 = X(X - 2)(X - 4)\) over \(\mathbb{Q}\). This elliptic curve has additive reduction at 2. One has \(E_8(\mathbb{Q})[2^\infty] = \{(0, 0), (2, 0), (4, 0), \infty\}\), and this group is isomorphic to \(V_4\). All torsion points, except \(\infty\), map to the singular point of the reduction. In fact, over \(\mathbb{Q}_2\), the points of good reduction are isomorphic to the group \(\mathbb{Z}_2\).

Sometimes, we can use Theorem \[\text{1}\] to show that rational points have infinite order.

**Example 18.** Consider the curve \(E_9 : Y^2 = X^3 - 2\) over \(\mathbb{Q}\). This curve has additive reduction at 2 and the point \((3, 5)\) has good reduction. By Theorem \[\text{1}\] the point has infinite order. Similarly, one can consider \(E_{10} : Y^2 = X^3 + 3\), which has additive reduction at 3. The point \((1, 2)\) has good reduction and infinite order by Theorem \[\text{1}\].
One can generalize the results above slightly. Starting with a torsion free \( E_i(K) \) such that \( pE_i(K) = E_{i+e}(K) \), one can use Lemma 7 to check if there is no torsion in \( E_{i-1}(K) \).

One of the problems in our construction, is that in general, even if \( E_i(K) \) is torsion free, it is not true that \( pE_i(K) = E_{i+e}(K) \), and hence our methods do not work directly. To do computations in this case, one needs to really compute the logarithm maps giving the isomorphism with \( m_i^1 \). We will give a brief example in which we study a ramified case.

**Example 19.** Take \( K = \mathbb{Q}_2(\sqrt{2}) \). One has \( k = \mathbb{F}_2 \) and \( m_K = \sqrt{2}\mathbb{Z}_2[\sqrt{2}] \). One has an exact sequence \( 0 \to E_1(K) \to E_0(K) \to k \to 0 \). One has \( E_i(K) \cong m_i^1 \) for \( i \geq 1 \) (Proposition 10). A computation gives \([2](T) = 2T - a_1T^2 + (a_1a_2 - 7a_3)T^4 + \ldots \). This polynomial induces a map \( g : k \to \widehat{E}(m_1^1)/\widehat{E}(m_3^1) \), and the latter group is isomorphic to \( m_K/m_3^K \) by a logarithm map. The map \( k \to m_K/m_3^K \) is of the form \( s \mapsto (\sqrt{2}c_0 + 2c_1)s \) with \( c_0, c_1 \in \{0, 1\} \). Unfortunately, one needs the logarithm map explicitly to see which map this is in terms of the \( a_i \). One then uses Lemma 7 to describe the torsion of \( E_0(K) \).

If there is no torsion, one can describe \( E_0(K) \) as a subgroup of \( K \).

| \( c_0 \) | \( c_1 \) | \( \text{im}(g) \) | \( \ker(g) \) | \( E_0(K) \) | \( E_0(K)[2] \) |
|-------|-------|-------------|-------------|-------------|-------------|
| 0     | 0     | \{0\} = m_3^4/m_3^K | \( k \) | \( - \) | \( \mathbb{Z}/2\mathbb{Z} \) |
| 0     | 1     | \{0, 2\} = m_2^3/m_3^K | \( 0 \) | \( \mathcal{O}_K \) | \( 0 \) |
| 1     | 0     | \{0, \sqrt{2}\} | \( 0 \) | \( 1\sqrt{2}\mathbb{Z}_p \oplus 2\mathbb{Z}_p \) | \( 0 \) |
| 1     | 1     | \{0, \sqrt{2} + 2\} | \( 0 \) | \( (1/\sqrt{2} + 1)\mathbb{Z}_p \oplus 2\mathbb{Z}_p \) | \( 0 \) |

Without explicit computations of the logarithm, one cannot distinguish between the third and fourth option. In the cases \((c_0, c_1) = (1, 0), (1, 1), E_0(K) \) is not identified with \( \mathcal{O}_K \) and hence \( pE_0(K) \neq E_2(K) \).

## 4 Acknowledgements

It is a pleasure to thank Ronald van Luijk and Sir Peter Swinnerton-Dyer for many useful remarks.

## References

[1] René Pannekoek. On \( p \)-torsion of \( p \)-adic elliptic curves with additive reduction. [arXiv:1211.5833](https://arxiv.org/abs/1211.5833)

[2] Joseph H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics*. Springer, Dordrecht, second edition, 2009.

[3] Peter Swinnerton-Dyer. Density of rational points on certain surfaces. *Algebra Number Theory*, 7(4):835–851, 2013.