On $p$-torsion of $p$-adic elliptic curves with additive reduction

René Pannekoek

May 5, 2014

1 Introduction

In this article, we fix a prime $p$. If $E/\mathbb{Q}_p$ is an elliptic curve with additive reduction, and one chooses for it a minimal Weierstrass equation over $\mathbb{Z}_p$:

$$y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6, \quad a_i \in \mathbb{Z}_p \text{ for each } i,$$

then we denote by $E_0(\mathbb{Q}_p) \subset E(\mathbb{Q}_p)$ the subgroup of points that reduce to a non-singular point of the reduced curve. As is well-known, this subgroup does not depend on the choice of minimal Weierstrass equation.

The purpose of this note is to investigate the structure of $E_0(\mathbb{Q}_p)$ as a topological group.

**Theorem 1.** Let $E/\mathbb{Q}_p$ be an elliptic curve with additive reduction, such that it can be given by a minimal Weierstrass equation over $\mathbb{Z}_p$:

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

where the $a_i$ are contained in $p\mathbb{Z}_p$ for each $i$. Then the group $E_0(\mathbb{Q}_p)$ is topologically isomorphic to $\mathbb{Z}_p$, except in the following four cases:

1. $p = 2$ and $a_1 + a_3 \equiv 2 \pmod{4}$;
2. $p = 3$ and $a_2 \equiv 6 \pmod{9}$;
3. $p = 5$ and $a_4 \equiv 10 \pmod{25}$;
4. $p = 7$ and $a_6 \equiv 14 \pmod{49}$.

In each of the cases (i)-(iv), $E_0(\mathbb{Q}_p)$ is topologically isomorphic to $p\mathbb{Z}_p \times \mathbb{F}_p$, where $\mathbb{F}_p$ has the discrete topology.
The proof of Theorem 1 will be given in Section 4.5. The case \( p > 7 \) of Theorem 1 was also mentioned in [3].

We will say a few words about the idea of the proof. It is a standard fact from the theory of elliptic curves over local fields [2, VII.6.3] that \( E_0(\mathbb{Q}_p) \) admits a canonical filtration

\[
E_0(\mathbb{Q}_p) \supset E_1(\mathbb{Q}_p) \supset E_2(\mathbb{Q}_p) \supset E_3(\mathbb{Q}_p) \supset \ldots,
\]

where for each \( i \geq 1 \) the quotient \( E_i(\mathbb{Q}_p)/E_{i+1}(\mathbb{Q}_p) \) is isomorphic to \( \mathbb{F}_p \). The quotient \( E_0(\mathbb{Q}_p)/E_1(\mathbb{Q}_p) \) is also isomorphic to \( \mathbb{F}_p \) by the fact that \( E \) has additive reduction. One has a natural isomorphism of topological groups \( j : E_2(\mathbb{Q}_p) \sim \mathbb{p}^2 \mathbb{Z}_p \) given by the theory of formal groups. If \( p > 2 \), the same theory even gives a natural isomorphism \( j' : E_1(\mathbb{Q}_p) \sim \mathbb{p} \mathbb{Z}_p \). These isomorphisms identify \( E_n(\mathbb{Q}_p) \) with \( \mathbb{p}^n \mathbb{Z}_p \) for all \( n \geq 2 \). The idea of the proof of theorem 1 is to start from \( j \) or \( j' \) and, by extending its domain, to build up an isomorphism between \( E_0(\mathbb{Q}_p) \) and either \( \mathbb{Z}_p \) or \( \mathbb{p} \mathbb{Z}_p \times \mathbb{F}_p \).

Rather than elliptic curves over \( \mathbb{Q}_p \) with additive reduction, we consider the more general case of Weierstrass curves over \( \mathbb{Z}_p \) whose generic fiber is smooth and whose special fiber is a cuspidal cubic curve. This allows more general results. Theorem 1 is derived as a special case.

At the end of the note, we give examples for each prime \( 2 \leq p \leq 7 \) of an elliptic curve \( E/\mathbb{Q} \) with additive reduction at \( p \) such that \( E_0(\mathbb{Q}_p) \) contains a \( p \)-torsion point defined over \( \mathbb{Q} \).

## 2 Preliminaries

### 2.1 Preliminaries on Weierstrass curves

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

Let \( K \) be a finite field extension of \( \mathbb{Q}_p \) for some prime \( p \), and 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 \( \mathcal{E} \subset \mathbb{P}^2_{\mathcal{O}_K} \) 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 \( \mathcal{E}_K \) is an elliptic curve with \((0 : 1 : 0)\) as the origin. The coefficients \( a_i \) are uniquely determined by \( \mathcal{E} \). The discriminant of \( \mathcal{E} \), denoted \( \Delta_\mathcal{E} \), is defined as in [2, III.1]. The curve \( \mathcal{E} \) is said to be minimal if \( v_K(\Delta_\mathcal{E}) \) is minimal among \( v_K(\Delta_{\mathcal{E}'}) \), where \( \mathcal{E}' \) ranges over the Weierstrass curves such that \( \mathcal{E}'_K \cong \mathcal{E}_K \).

We will say that a Weierstrass curve \( \mathcal{E}/\mathcal{O}_K \) has **good reduction** when the special fiber \( \mathcal{E}_k \) is smooth, **multiplicative reduction** when \( \mathcal{E}_k \) is nodal (i.e. there are two distinct tangent directions to the singular point), and **additive reduction** when \( \mathcal{E}_k \) is cuspidal (i.e. one tangent direction to the singular point). A non-minimal Weierstrass curve has additive reduction. The reduction type of an elliptic curve \( E \) is defined to be the reduction type
of a minimal Weierstrass model of $E$ over $\mathcal{O}_K$, which is a minimal Weierstrass curve $\mathcal{E}/\mathcal{O}_K$ such that $\mathcal{E}_K \cong E$. By the fact that the minimal Weierstrass model of $E$ is unique up to $\mathcal{O}_K$-isomorphism, this is well-defined.

We have $E(K) = \mathcal{E}(K) = \mathcal{E}(\mathcal{O}_K)$ since $\mathcal{E}$ is projective. Therefore, we have a reduction map $E(K) \to \mathcal{E}(k)$ given by restricting an element of $\mathcal{E}(\mathcal{O}_K)$ to the special fiber. By $\mathcal{E}_0(K)$ we denote the subgroup $\mathcal{E}_0(K) \subset \mathcal{E}(K)$ of points reducing to a non-singular point of the special fiber $\mathcal{E}_k$. By $\mathcal{E}_1(K) \subset \mathcal{E}_0(K)$ we denote the kernel of reduction, i.e. the points that map to the identity $0_k$ of $\mathcal{E}(k)$. A more explicit definition of $\mathcal{E}_1(K)$ is

$$
\mathcal{E}_1(K) = \{(x, y) \in \mathcal{E}(K) : v_K(x) \leq -2, v_K(y) \leq -3\} \cup \{0\}.
$$

(2)

More generally, one defines subgroups $\mathcal{E}_n(K) \subset \mathcal{E}_0(K)$ as follows:

$$
\mathcal{E}_n(K) = \{(x, y) \in \mathcal{E}(K) : v_K(x) \leq -2n, v_K(y) \leq -3n\} \cup \{0\}.
$$

We thus have an infinite filtration on the subgroup $\mathcal{E}_1(K)$:

$$
\mathcal{E}_1(K) \supset \mathcal{E}_2(K) \supset \mathcal{E}_3(K) \supset \cdots
$$

(3)

For an elliptic curve $E/K$ and an integer $n \geq 0$, we define $E_n(K)$ to be $\mathcal{E}_n(K)$, where $\mathcal{E}$ is a minimal Weierstrass model of $E$ over $\mathcal{O}_K$. The $E_n(K)$ are well-defined, again by the fact that the minimal Weierstrass model of $E$ is unique up to $\mathcal{O}_K$-isomorphism.

**Proposition 2.** For $\mathcal{E}$ a Weierstrass curve over $\mathbb{Z}_p$, there is an exact sequence

$$
0 \to \mathcal{E}_1(K) \to \mathcal{E}_0(K) \to \tilde{\mathcal{E}}_{\text{sm}}(k) \to 0,
$$

where $\tilde{\mathcal{E}}_{\text{sm}}$ is the complement of the singular points in the special fiber $\tilde{\mathcal{E}}$.

**Proof.** This comes down to Hensel’s lemma. See [2, VII.2.1].

For any Weierstrass curve $\mathcal{E}$, we can consider its formal group $\hat{\mathcal{E}}$ [2 IV.1–2]. This is a one-dimensional formal group over $\mathcal{O}_K$. Giving the data of this formal group is the same as giving a power series $F = F_{\hat{\mathcal{E}}}$ in $\mathcal{O}_K[[X,Y]]$, 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 $\mathcal{E}$ as in (1), the first few terms of $F$ are given by:

$$
F(X,Y) = X + Y - a_1 XY - a_2 (X^2 Y + XY^2) - 2a_3 (X^3 Y + XY^3) + (a_1 a_2 - 3a_3)X^2 Y^2 - (2a_1 a_3 + 2a_4)(X^4 Y + XY^4) - (a_1 a_3 - a_2^2 + 4a_4)(X^3 Y^2 + X^2 Y^3) + \ldots
$$

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 \( \text{wt} \), such that \( \text{wt}(a_i) = i \) for each \( i \), then the coefficients of \( F \) in degree \( n \) are homogeneous of weight \( n - 1 \) \([2, \text{IV.1.1}]. \) For each \( n \in \mathbb{Z}_{\geq 2} \), we define power series \( [n] \) in \( \mathcal{O}_K[[T]] \) 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 \( \mathcal{O}_K[[T]] \) 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 3.** Let \( [p] = \sum_n b_n T^n \in \mathbb{Z}[a_1, a_2, a_3, a_4, a_6][[T]] \) be the generic formal multiplication by \( p \) law. Then:

1. \( p \mid b_n \) for all \( n \) not divisible by \( p \);
2. \( \text{wt}(b_n) = n - 1 \), considering \( \mathbb{Z}[a_1, a_2, a_3, a_4, a_6] \) as a weighted ring as above.

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

The series \( F(u, v) \) converges to an element of \( \mathfrak{m}_K \) for all \( u, v \in \mathfrak{m}_K \). To \( \mathcal{E} \) one associates the group \( \hat{\mathcal{E}}(\mathfrak{m}_K) \), the \( \mathfrak{m}_K \)-valued points of \( \hat{\mathcal{E}} \), which as a set is just \( \mathfrak{m}_K \), and whose group operation + is given by \( u + v = F(u, v) \) for all \( u, v \in \hat{\mathcal{E}}(\mathfrak{m}_K) \). The identity element of \( \hat{\mathcal{E}}(\mathfrak{m}_K) \) is \( 0 \in \mathfrak{m}_K \). If \( n \geq 1 \) is an integer, then by \( \hat{\mathcal{E}}(\mathfrak{m}_K^n) \) we denote the subset of \( \hat{\mathcal{E}}(\mathfrak{m}_K) \) corresponding to the subset \( \mathfrak{m}_K^n \subset \mathfrak{m}_K \), where \( \mathfrak{m}_K^n \) is the \( n \)th power of the ideal \( \mathfrak{m}_K \) of \( \mathcal{O}_K \). The groups \( \hat{\mathcal{E}}(\mathfrak{m}_K^n) \) are subgroups of \( \hat{\mathcal{E}}(\mathfrak{m}_K) \), and we have an infinite filtration of \( \hat{\mathcal{E}}(\mathfrak{m}_K) \):

\[
\hat{\mathcal{E}}(\mathfrak{m}_K) \supset \hat{\mathcal{E}}(\mathfrak{m}_K^2) \supset \hat{\mathcal{E}}(\mathfrak{m}_K^3) \supset \cdots \tag{4}
\]

**Proposition 4.** The map

\[
\psi_K : \mathcal{E}_1(K) \xrightarrow{\sim} \hat{\mathcal{E}}(\mathfrak{m}_K)
\]

\[
(x, y) \mapsto -x/y
\]

\[
0 \mapsto 0
\]

is an isomorphism of topological groups. Moreover, \( \psi_K \) respects the filtrations \([3]\) and \([4]\), i.e. it identifies the subgroups \( \mathcal{E}_n(K) \) defined above with \( \hat{\mathcal{E}}(\mathfrak{m}_K^n) \).

**Proof.** See \([2, \text{VII.2.2}]\).
Proof. First, we claim that \( \text{Ext}^1_{\mathbb{Z}} \) results in the exact sequence
\[
\text{exact sequence associated to } \text{Hom}_{\mathbb{Z}} \]
where the last equality follows from the fact that \( \text{Hom}(\mathbb{Z}, X) \) isomorphic as a topological group to either \( \mathbb{Z} \) or \( \mathbb{Z} \times F_p \). Here \( \hat{\mathbb{Z}} \) which proves the claim. Putting \( A = \mathbb{Z}/p \mathbb{Z} \), we find \( \text{Ext}^1_{\mathbb{Z}}(F_p, A) = \mathbb{A}/pA \). Then \( \mathbb{Z} \) endowed with the indiscrete topology.

Proposition 5. Suppose \( X \) is a topological abelian group and we have a short exact sequence
\[
0 \to \mathbb{Z}_p^d \to X \to F_p \to 0.
\]
of topological groups where the second arrow is a topological embedding. Then \( X \) is isomorphic as a topological group to either \( \mathbb{Z}_p^d \) or \( \mathbb{Z}_p^d \times F_p \). It is indeed necessary to require \( \mathbb{Z}_p^d \to X \) to be a topological embedding, i.e. a homeomorphism onto its image, since otherwise we could take \( X \) to be the product \( (\mathbb{Z}_p^d)^{\text{ind}} \times F_p \), where the first factor is the abelian group \( \mathbb{Z}_p^d \) endowed with the indiscrete topology.

Proof. First, we claim that \( \text{Ext}^1_{\mathbb{Z}}(F_p, A) = \mathbb{A}/pA \) for any abelian group \( A \). Taking the long exact sequence associated to \( \text{Hom}_{\mathbb{Z}}(-, A) \) for the exact sequence \( 0 \to \mathbb{Z} \xrightarrow{p} \mathbb{Z} \to F_p \to 0 \) results in the exact sequence
\[
\text{Hom}(\mathbb{Z}, A) \to \text{Hom}(\mathbb{Z}, A) \to \text{Ext}^1_{\mathbb{Z}}(F_p, A) \to \text{Ext}^1_{\mathbb{Z}}(\mathbb{Z}, A) = 0
\]
where the last equality follows from the fact that \( \text{Hom}(\mathbb{Z}, -) \) is an exact functor. Using that \( \text{Hom}(\mathbb{Z}, A) = A \), we get
\[
\text{Ext}^1_{\mathbb{Z}}(F_p, A) = A/pA,
\]
which proves the claim. Putting \( A = \mathbb{Z}_p^d \), we find \( \text{Ext}^1_{\mathbb{Z}}(F_p, \mathbb{Z}_p^d) = \mathbb{F}_p^d \). We conclude that the equivalence classes of extensions of \( \mathbb{Z} \)-modules \( 0 \to \mathbb{Z}_p^d \to X \to F_p \to 0 \) are in bijective correspondence with the elements of \( \mathbb{F}_p^d \). The element \( 0 \in \mathbb{F}_p^d \) corresponds to the split extension. The non-split ones are obtained as follows. For \( v \in \mathbb{Z}_p^d - p\mathbb{Z}_p^d \), we construct an extension
\[
0 \to \mathbb{Z}_p^d \to X_v \xrightarrow{f_v} F_p \to 0
\]
by defining the subgroup \( X_v \subset \mathbb{O}_p^d \) as \( X_v = \mathbb{Z}_p^d + \langle v/p \rangle \) and letting \( f_v : X_v \to F_p \) be the unique group homomorphism that is trivial on \( \mathbb{Z}_p^d \subset X_v \) and that sends \( v/p \) to 1. The equivalence class of the above extension only depends on the class of \( v \) modulo \( p \mathbb{Z}_p^d \). Note that if we take any element \( x \in X_v \) mapping to 1 in \( F_p \), we have \( px = v + pv_1 \in \mathbb{Z}_p^d \) for some \( v_1 \in \mathbb{Z}_p^d \). Note further that \( X_v \) is topologically isomorphic to \( \mathbb{Z}_p^d \), if we give it the subspace topology.

A diagram chase shows that this construction gives us \( p^d - 1 \) different equivalence classes of extensions. Suppose that \( v, w \in \mathbb{Z}_p^d - p\mathbb{Z}_p^d \) and \( \phi : X_v \xrightarrow{\sim} X_w \) are such that
\[
\begin{array}{ccccccccc}
0 & \longrightarrow & \mathbb{Z}_p^d & \longrightarrow & X_v & \xrightarrow{f_v} & F_p & \longrightarrow & 0 \\
\text{id} & & \downarrow & & \phi & & \downarrow & & \text{id} \\
0 & \longrightarrow & \mathbb{Z}_p^d & \longrightarrow & X_w & \xrightarrow{f_w} & F_p & \longrightarrow & 0
\end{array}
\]
is a commutative diagram. Consider an element \( x \in X_v \) such that \( f_v(x) = 1 \). Then \( f_w(\phi(x)) = 1 \). Furthermore, \( px = v + pv_1 \) for some \( v_1 \in p\mathbb{Z}_p^d \), and \( \phi(px) = p\phi(x) = w + pw_1 \) for some \( w_1 \in p\mathbb{Z}_p^d \). Hence \( v + pv_1 = \phi(v + pv_1) = w + pw_1 \), so \( v \equiv w \) (mod \( p\mathbb{Z}_p^d \)).

Let \( X \) be a topological group sitting inside an extension of topological groups \( 0 \to \mathbb{Z}_p^d \xrightarrow{i} X \xrightarrow{f} \mathbb{F}_p \to 0 \), with \( i \) a topological embedding and \( f \) continuous. This means that there exists an extension of topological groups \( 0 \to \mathbb{Z}_p^d \to Y \to \mathbb{F}_p \to 0 \) that is either split or equal to one of the form \( 0 \to \mathbb{Z}_p^d \to X_v \xrightarrow{f} \mathbb{F}_p \to 0 \), an isomorphism of groups \( \phi : X \xrightarrow{\sim} Y \), and a commutative diagram:

\[
\begin{array}{ccc}
0 & \to & \mathbb{Z}_p^d \\
\downarrow & & \downarrow \phi \\
0 & \to & \mathbb{Z}_p^d \\
\end{array}
\begin{array}{ccc}
& \xrightarrow{f} & \mathbb{F}_p \\
& \downarrow \text{id} & \downarrow \text{id} \\
& \mathbb{F}_p & \to 0.
\end{array}
\]

We claim that \( \phi \) must also be a homeomorphism. Since both \( X \) and \( Y \) are topological disjoint unions of the translates of their subgroups \( \mathbb{Z}_p^d \), and \( \phi \) respects the disjoint union decomposition, this is clear. So \( X \) is topologically isomorphic to \( Y \), and hence to either \( \mathbb{Z}_p^d \) or \( \mathbb{Z}_p^d \times \mathbb{F}_p \).

**Remark 6.** By repeatedly applying Proposition 5 we see that if we have a finite filtration \( \mathbb{Z}_p^d = M_n \subset M_{n-1} \subset \ldots \subset M_1 \) of topological groups, in which all quotients are isomorphic to \( \mathbb{F}_p \), then \( M_1 \) is torsion-free if and only if it is topologically isomorphic to \( \mathbb{Z}_p^d \).

The following is a strengthening of Proposition 5 in the case \( d = 1 \), which will be important for us.

**Corollary 7.** Let \( p \) be a prime and suppose we have a short exact sequence

\[ 0 \to p\mathbb{Z}_p \xrightarrow{i} X \to \mathbb{F}_p \to 0 \]

of topological abelian groups where the second arrow is a topological embedding. If \( X \) is topologically isomorphic to \( \mathbb{Z}_p \), then \( v_p(i^{-1}(px)) = 1 \) for all \( x \in X - i(p\mathbb{Z}_p) \), where \( v_p \) is the \( p \)-adic valuation. If \( X \) is not topologically isomorphic to \( \mathbb{Z}_p \), it is topologically isomorphic to \( p\mathbb{Z}_p \times \mathbb{F}_p \), and we have \( v_p(i^{-1}(px)) > 1 \) for all \( x \in X - i(p\mathbb{Z}_p) \).

**Proof.** If \( X \) is topologically isomorphic to \( \mathbb{Z}_p \), the map \( i \) is given by multiplication by some unit \( \alpha \in \mathbb{Z}_p^* \) followed by the inclusion \( p\mathbb{Z}_p \subset \mathbb{Z}_p \). The conclusion follows.

If \( X \) is not topologically isomorphic to \( \mathbb{Z}_p \), then by Proposition 5 we must have \( X \cong p\mathbb{Z}_p \times \mathbb{F}_p \). But then if \( x = (y,c) \), we have \( v_p(i^{-1}(px)) = v_p(py) > 1 \).
Lemma 8. Let $K$ be a finite extension of $\mathbb{Q}_p$ with ring of integers $\mathcal{O}_K$. Then $\mathcal{O}_K$ is topologically isomorphic to $\mathbb{Z}_p^d$, where $d = [K : \mathbb{Q}_p]$.

Proof. $\mathcal{O}_K$ is a free $\mathbb{Z}_p$-module of rank $d$, so there is a group isomorphism $\mathbb{Z}_p^d \sim \mathcal{O}_K$. Since both groups are topologically finitely generated, any isomorphism between them is bicontinuous [1, 1.1].

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

As in section 2, let $K$ be a finite extension of $\mathbb{Q}_p$. Let $\mathcal{O}_K$ again be the ring of integers of $K$, with maximal ideal $m_K$ and residue field $k$.

In this section, we gather some general properties of Weierstrass curves over $\mathcal{O}_K$ with additive reduction.

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

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

where all $a_i$ lie in $m_K$.

Proof. We construct an automorphism $\alpha \in \text{PGL}_3(\mathcal{O}_K)$ that maps $\mathcal{E}$ 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 $\mathcal{E}_k$ to $(0 : 0 : 1)$. The image $\mathcal{E}_1 = \alpha_1(\mathcal{E})$ is a Weierstrass curve with coefficients satisfying $a_3, a_4, a_6$ in $m_K$. 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 $\alpha_2(\mathcal{E}_1)$ the unique tangent at $(0 : 0 : 1)$ is given by $y' = 0$. The Weierstrass curve $\mathcal{E}_2 = \alpha_2(\mathcal{E}_1)$ now has all its coefficients $a_1, a_2, a_3, a_4, a_6$ in $m_K$. One may thus take $\alpha = \alpha_2 \circ \alpha_1$. □

Suppose that $\mathcal{E}/\mathcal{O}_K$ is a Weierstrass curve given by (1), and suppose that the $a_i$ are contained in $m_K$. In particular, $\mathcal{E}$ has additive reduction. If we let $F$ denote the formal group law of $\mathcal{E}$, 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 $\hat{\mathcal{E}}(m_K)$. The same statement holds true when we replace $K$ by a finite field extension $L$.

Definition 10. Let $\mathcal{E}/\mathcal{O}_K$ be a Weierstrass curve given by (1), and assume that the $a_i$ are contained in $m_K$. For any finite field extension $K \subset L$, we denote by $\hat{\mathcal{E}}(\mathcal{O}_L)$ the topological group obtained by endowing the space $\mathcal{O}_L$ with the group structure induced by $F$.

The following proposition will be fundamental in determining of the structure of $\mathcal{E}_0(\mathbb{Q}_p)$ as a topological group for Weierstrass curves with additive reduction.
Proposition 11. Let $\mathcal{E}/\mathcal{O}_K$ be a Weierstrass curve given by (1), and assume that the $a_i$ are contained in $m_K$.

1. The map $\Psi : \mathcal{E}_0(K) \to \hat{\mathcal{E}}(\mathcal{O}_K)$ that sends $(x,y)$ to $-x/y$ is an isomorphism of topological groups.

2. If $6e(K/Q_p) < p - 1$, where $e$ denotes the ramification degree, then $\mathcal{E}_0(K)$ is also topologically isomorphic to $\mathcal{O}_K$ equipped with the usual group structure.

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

$$y^2 + \alpha_1 xy + \alpha_3 y = x^3 + \alpha_2 x^2 + \alpha_4 x + \alpha_6,$$

where $\alpha_i = a_i/\rho^i$. There is a birational map $\phi : \mathcal{E} \times_{\mathcal{O}_K} \mathcal{O}_L \to D$, 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 $\mathcal{E}(L)$ and $D(L)$. Using (2) and the fact that we have $(x, y) \in \mathcal{E}_0(L)$ if and only if $v_L(x), v_L(y)$ are both not greater than zero, one sees that $\phi$ induces a bijection $\mathcal{E}_0(L) \sim \mathcal{D}_1(L)$, that all maps (a priori just of sets) in the following diagram are well-defined, and that the diagram commutes:

$$\begin{array}{cccccc}
\mathcal{E}_1(K) & \overset{\text{incl}}{\longrightarrow} & \mathcal{E}_0(K) & \overset{\text{incl}}{\longrightarrow} & \mathcal{E}_0(L) & \overset{\phi}{\longrightarrow} & \mathcal{D}_1(L) \\
\downarrow \psi_K & & \downarrow \psi & & \downarrow \psi_L & & \downarrow \psi_L \\
\hat{\mathcal{E}}(m_K) & \overset{\text{incl}}{\longrightarrow} & \hat{\mathcal{E}}(\mathcal{O}_K) & \overset{\text{incl}}{\longrightarrow} & \hat{\mathcal{E}}(\mathcal{O}_L) & \overset{\rho}{\longrightarrow} & \hat{\mathcal{D}}(m_L)
\end{array}$$

Here the map $\psi_L : \mathcal{E}_0(L) \to \mathcal{O}_L$ 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. Note that the horizontal and vertical outer maps are all continuous. Since $\psi_L$, $\phi$ and multiplication by $\rho$ are homeomorphisms (for $\psi_L$ one uses Proposition 4), so is $\Psi_L$. Hence $\Psi$ must be a homeomorphism onto its image. By Galois theory, $\Psi$ is surjective, so it is itself a homeomorphism.

Let $F_\hat{D}$ be the formal group law of $D$. One calculates that

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

Hence all maps in the diagram are group homomorphisms. This proves the first part of the proposition.

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 $\mathcal{E}_1(K)$ is topologically isomorphic to $m_K$, and $\mathcal{D}_1(L)$ to $m_L$. Since $\mathcal{E}$ has additive reduction, we have $\hat{\mathcal{E}}_{sm}(k) \cong k^+ \cong \mathbf{F}_p^f$, where $f = f(K/Q_p)$ is the inertia degree of $K/Q_p$ and $\hat{\mathcal{E}}_{sm}$ is the smooth locus of the special fiber of $\mathcal{E}$. Proposition 2 shows we have a short exact sequence

$$0 \to m_K \to \mathcal{E}_0(K) \to \mathbf{F}_p^f \to 0.$$
In the diagram above, the topological group $\mathcal{E}_0(K)$ is mapped homomorphically into the torsion-free group $\mathcal{D}_1(L)$, hence it is itself torsion-free. It follows from Remark 6 that $\mathcal{E}_0(K)$ is topologically isomorphic to $\mathcal{O}_K$. This proves the second part.

The following corollary is worth noting, but will not be used in what follows.

**Corollary 12.** Let $\mathcal{E}/\mathcal{O}_K$ be a Weierstrass curve with additive reduction. If $6e(K/Q_p) < p - 1$, then $\mathcal{E}_0(K)$ is topologically isomorphic to $\mathcal{O}_K$.

**Proof.** The statement that $\mathcal{E}_0(K)$ is topologically isomorphic to $\mathcal{O}_K$ only depends on the $\mathcal{O}_K$-isomorphism class of $\mathcal{E}$. By Lemma 9 there exists a Weierstrass curve $\mathcal{E}'$ with $a_i \in \mathfrak{m}_K$ that is $\mathcal{O}_K$-isomorphic to $\mathcal{E}$. Now apply Proposition 11 to $\mathcal{E}'$. \qed

### 4 Weierstrass curves with additive reduction over $\mathbb{Z}_p$

In this section, we gather some general properties of Weierstrass curves over $\mathbb{Z}_p$ with additive reduction and finish the proof of theorem 1.

**Lemma 13.** Let $\mathcal{E}/\mathbb{Z}_p$ be a Weierstrass curve with additive reduction. Then there exists a topological isomorphism $\chi : \hat{\mathcal{E}}(p\mathbb{Z}_p) \cong p\mathbb{Z}_p$ such that for $n \in \mathbb{Z}_{\geq 1}$, $\chi$ identifies $\hat{\mathcal{E}}(p^n\mathbb{Z}_p)$ with $p^n\mathbb{Z}_p$.

**Proof.** For $p > 2$, this is standard; the proof may be found in [2, IV.6.4(b)]. We now treat the case $p = 2$. By Lemma 9 we may assume that the Weierstrass coefficients $a_i$ of $\mathcal{E}$ all lie in $2\mathbb{Z}_2$. The multiplication by 2 on $\hat{\mathcal{E}}(2\mathbb{Z}_2)$ is given by the power series

$$[2](T) = F_{\hat{\mathcal{E}}}(T, T) = 2T - a_1T^2 - a_2T^3 + (a_1a_2 - 7a_3)T^4 - \ldots,$$

where $F_{\hat{\mathcal{E}}}$ is the formal group law of $\mathcal{E}$. By [2, IV.3.2(a)], $\hat{\mathcal{E}}(2\mathbb{Z}_2)/\hat{\mathcal{E}}(4\mathbb{Z}_2)$ is cyclic of order 2. By [2, IV.6.4(b)], there exists a topological isomorphism $\hat{\mathcal{E}}(4\mathbb{Z}_2) \cong 4\mathbb{Z}_2$. Hence there exists an extension

$$0 \to 2\mathbb{Z}_2 \xrightarrow{i} \hat{\mathcal{E}}(2\mathbb{Z}_2) \to \mathbb{Z}_2 \to 0.$$

From Theorem 5 we see that $\hat{\mathcal{E}}(2\mathbb{Z}_2)$ is topologically isomorphic either to $2\mathbb{Z}_2$ or to $4\mathbb{Z}_2 \times \mathbb{F}_2$. Assume that the latter is the case, then there is an element $z$ of order 2 in $\hat{\mathcal{E}}(2\mathbb{Z}_2)$ that is not contained in $\hat{\mathcal{E}}(4\mathbb{Z}_2)$. For such a $z$ we have $v_2(z) = 1$, where $v_2 : \hat{\mathcal{E}}(2\mathbb{Z}_2) \to \mathbb{Z}_{\geq 1} \cup \{\infty\}$ is the 2-adic valuation on the underlying set $2\mathbb{Z}_2$ of $\hat{\mathcal{E}}(2\mathbb{Z}_2)$. Using that in the duplication power series 3 we have $a_i \in 2\mathbb{Z}_2$ for each $i$, it follows that $v_2([2](z)) = 2$, so $[2](z) \neq 0$. This is a contradiction, so there exists an isomorphism $\chi : \hat{\mathcal{E}}(2\mathbb{Z}_2) \cong 2\mathbb{Z}_2$ as topological groups. From this, and from the fact that $\hat{\mathcal{E}}(2^n\mathbb{Z}_2)/\hat{\mathcal{E}}(2^{n+1}\mathbb{Z}_2) \cong \mathbb{F}_2$ for all $n \in \mathbb{Z}_{\geq 1}$ [2, IV.3.2(a)], we see that $\chi$ necessarily respects the filtrations on either side. \qed

**Corollary 14.** Let $\mathcal{E}/\mathbb{Z}_p$ be a Weierstrass curve with additive reduction. Then there exists an isomorphism $\mathcal{E}_1(\mathbb{Q}_p) \cong p\mathbb{Z}_p$ which for $n \in \mathbb{Z}_{\geq 1}$ identifies $\mathcal{E}_n(\mathbb{Q}_p)$ with $p^n\mathbb{Z}_p$.

**Proof.** Such an isomorphism can be obtained by composing the isomorphism $\chi$ from Lemma 13 with the isomorphism $\psi_{\mathbb{Q}_p}$ from Proposition 11. \qed
4.1 \( p = 2 \)

**Proposition 15.** Let \( E/\mathbb{Z}_2 \) be a Weierstrass curve with its coefficients \( a_i \) in \( 2\mathbb{Z}_2 \). Then \( E_0(\mathbb{Q}_2) \) is topologically isomorphic to \( \mathbb{Z}_2 \) if \( a_1 + a_3 \equiv 0 \pmod{4} \), and to \( 2\mathbb{Z}_2 \times F_2 \) otherwise.

**Proof.** Proposition 2 shows that there is a short exact sequence

\[
0 \to E_1(\mathbb{Q}_2) \to E_0(\mathbb{Q}_2) \to F_2 \to 0.
\]

By Lemma 13, we have \( E_1(\mathbb{Q}_2) \cong 2\mathbb{Z}_2 \), so Proposition 5 implies that \( E_0(\mathbb{Q}_2) \) is topologically isomorphic either to \( \mathbb{Z}_2 \) or to \( 2\mathbb{Z}_2 \times F_2 \).

Let \([2](T) \in O_K[[T]]\) be the formal duplication formula (5) on \( E \). Let \( \Psi \) be the map from Proposition 11. Since \( \Psi \) is an isomorphism of topological groups, we have for all \( P \in E_0(\mathbb{Q}_2) \):

\[
\Psi(2P) = [2](\Psi(P)).
\] (6)

By Corollary 7, we have \( E_0(\mathbb{Q}_2) \cong \mathbb{Z}_2 \) if and only if for all \( P \in E_0(\mathbb{Q}_2) - E_1(\mathbb{Q}_2) \) we have \( 2P = E_1(\mathbb{Q}_2) - E_2(\mathbb{Q}_2) \), which by (6) is true if and only if for all \( z \in \hat{E}(\mathbb{Z}_2) - \hat{E}(2\mathbb{Z}_2) \) we have \( v_2([2](z)) = 1 \), where \( v_2 : \hat{E}(\mathbb{Z}_2) \to \mathbb{Z}_{\geq 0} \cup \{\infty\} \) is the 2-adic valuation on the underlying set \( \mathbb{Z}_2 \) of \( \hat{E}(\mathbb{Z}_2) \). This condition may be checked using the duplication power series

\[
[2](T) = 2T - a_1T^2 - 2a_2T^3 + (a_1a_2 - 7a_3)T^4 - \ldots = \sum_{i=1}^{\infty} b_iT^i.
\]

In deciding whether \( v_2([2](z)) = 1 \) for \( z \in \hat{E}(\mathbb{Z}_2) - \hat{E}(2\mathbb{Z}_2) \), we do not need to consider those parts of terms whose coefficients have valuation \( \geq 2 \). The non-linear parts of each coefficient \( b_i \) will contribute only terms with valuation \( \geq 2 \), so may ignore these and keep only the linear parts. The terms \( b_i z^i \) with \( i \) odd we may discard altogether; by Lemma 3 all their coefficients have valuation \( \geq 2 \). Finally, we may discard all terms \( b_i z^i \) with \( i \) even and \( \geq 6 \): a polynomial in \( \mathbb{Z}[a_1, \ldots, a_6] \) whose weight is odd and at least 5 does not contain a linear term (there being no \( a_5 \)), so the terms involving \( z^6, z^8, z^{10}, \ldots \) will have valuation \( \geq 2 \).

We thus get that, if \( z \in \hat{E}(\mathbb{Z}_2) - \hat{E}(2\mathbb{Z}_2) \),

\[
v_2([2](z)) = 1 \iff v_2(2z - a_1z^2 - 7a_3z^4) = 1.
\]

This is true for all \( z \in \hat{E}(\mathbb{Z}_2) - \hat{E}(2\mathbb{Z}_2) \) if and only if:

\[
v_2(z - \frac{a_1}{2}z^2 - \frac{7a_3}{2}z^4) = 0 \iff a_1 + 7a_3 \equiv 0 \pmod{4} \iff a_1 + a_3 \equiv 0 \pmod{4}
\]

since \( z \equiv z^2 \equiv z^4 \pmod{2} \). This proves the proposition. \( \square \)
4.2 $p = 3$

**Proposition 16.** Let $\mathcal{E}/\mathbb{Z}_3$ be a Weierstrass curve with its coefficients $a_i$ in $3\mathbb{Z}_3$. Then $\mathcal{E}_0(\mathbb{Q}_3)$ is topologically isomorphic to $\mathbb{Z}_3$ if $a_2 \not\equiv 6 \pmod{9}$, and to $3\mathbb{Z}_3 \times \mathbb{F}_3$ otherwise.

**Proof.** We proceed as in the proof of Proposition 15 using the formal triplication formula:

$$[3](T) = 3T - 3a_1T^2 + (a_1^2 - 8a_2)T^3 + (12a_1a_2 - 39a_3)T^4 + \ldots = \sum_{i=1}^{\infty} b_i T^i. \quad (7)$$

We consider the usual exact sequence for $\mathcal{E}_0(\mathbb{Q}_3)$:

$$0 \to \mathcal{E}_1(\mathbb{Q}_3) \to \mathcal{E}_0(\mathbb{Q}_3) \to \mathbb{F}_3 \to 0.$$ 

We see from $\mathcal{E}_1(\mathbb{Q}_3) \cong 3\mathbb{Z}_3$ and Corollary 4 that $\mathcal{E}_0(\mathbb{Q}_3)$ is topologically isomorphic to $3\mathbb{Z}_3 \times \mathbb{F}_3$ if and only if for all elements $z \in \hat{\mathcal{E}}(\mathbb{Z}_3) - \hat{\mathcal{E}}(3\mathbb{Z}_3)$, $[3](z)$ has valuation greater than 1. On the other hand, $\mathcal{E}_0(\mathbb{Q}_3)$ is topologically isomorphic to $\mathbb{Z}_3$ if for all such $z$, the valuation of $[3](z)$ is 1. Reasoning as in the proof of Proposition 15 we see that we may ignore all terms of degree not equal to 1 or a multiple of 3 since their coefficients are divisible by 3 and have positive weight. Also we may ignore the terms of degree both equal to a multiple of 3 and greater than 3, since their coefficients do not contain parts that are linear in $a_1, \ldots, a_6$. Finally, we may ignore the non-linear part of the term of degree 3. We see that for $z \in \hat{\mathcal{E}}(\mathbb{Z}_3) - \hat{\mathcal{E}}(3\mathbb{Z}_3)$, we have:

$$v_3([3](z)) = 1 \iff v_3(3z - 8a_2z^3) = 1.$$ 

This happens for all such $z$ if and only if:

$$v_3(z - \frac{8a_2}{3}z^3) = 0 \iff 1 - \frac{8a_2}{3} \not\equiv 0 \pmod{3} \iff a_2 \not\equiv 6 \pmod{9}$$

since $z \equiv z^3 \pmod{3}$. This proves the proposition. \[\square\]

4.3 $p = 5$

**Proposition 17.** Let $\mathcal{E}/\mathbb{Z}_5$ be a Weierstrass curve with its coefficients $a_i$ in $5\mathbb{Z}_5$. Then $\mathcal{E}_0(\mathbb{Q}_5)$ is topologically isomorphic to $\mathbb{Z}_5$ if $a_4 \not\equiv 10 \pmod{25}$, and to $5\mathbb{Z}_5 \times \mathbb{F}_5$ otherwise.

**Proof.** For simplicity, we give the formal multiplication by 5 power series in the case where $a_1, a_2, a_3$ are zero:

$$[5](T) = 5T - 1248a_4T^5 + \ldots = \sum_{i=1}^{\infty} b_i T^i \quad (8)$$

This formula suffices for our purposes, since the same arguments as in the proofs of Propositions 15 and 16 show that the terms that are canceled by setting $a_1 = a_2 = a_3 = 0$ could have been ignored anyway.
We apply Corollary 7 to:

$$0 \rightarrow 5\mathbb{Z} \rightarrow \mathcal{E}_0(\mathbb{Q}_5) \rightarrow \mathbb{F}_5 \rightarrow 0.$$ In (8) we may ignore terms of degree not equal to 1 or 5, by the same reasoning as in the proofs of Propositions 13 and 16. We see that for $$z \in \hat{\mathcal{E}}(\mathbb{Z}_5) - \hat{\mathcal{E}}(5\mathbb{Z}_5)$$ we have:

$$v_5([5](z)) = 1 \iff v_5(5z - 1248a_4z^5) = 1.$$ This happens for all such $$z$$ if and only if:

$$v_5(z - \frac{1248a_4}{5}z^5) = 0 \iff 1 - \frac{1248a_4}{5} \not\equiv 0 \pmod{5} \iff a_4 \not\equiv 10 \pmod{25}$$ since $$z \equiv z^5 \pmod{5}$$. This proves the proposition.

4.4 $$p = 7$$

**Proposition 18.** Let $$\mathcal{E}/\mathbb{Z}_7$$ be a Weierstrass curve with its coefficients $$a_i$$ in $$7\mathbb{Z}_7$$. Then $$\mathcal{E}_0(\mathbb{Q}_7)$$ is topologically isomorphic to $$\mathbb{Z}_7$$ if $$a_6 \not\equiv 14 \pmod{49}$$, and to $$7\mathbb{Z}_7 \times \mathbb{F}_7$$ otherwise.

**Proof.** For simplicity, we give the formal multiplication by 7 power series with $$a_1, a_2, a_3$$ set to zero:

$$[7](T) = 7T - 6720a_4T^5 - 352944a_6T^7 + \ldots$$

As before, the terms that have disappeared as a result could have been ignored anyway. We apply Corollary 7 to:

$$0 \rightarrow 7\mathbb{Z}_7 \rightarrow \mathcal{E}_0(\mathbb{Q}_7) \rightarrow \mathbb{F}_7 \rightarrow 0.$$ In (9) we may ignore terms of degree not equal to 1 or 7, by the same reasoning as in the proofs of Propositions 13 and 16. We see that for $$z \in \hat{\mathcal{E}}(\mathbb{Z}_7) - \hat{\mathcal{E}}(7\mathbb{Z}_7)$$ we have:

$$v_7([7](z)) = 1 \iff v_7(7z - 352944a_6z^7) = 1.$$ This happens if and only if:

$$v_7(z - \frac{352944a_6}{7}z^7) = 0 \iff 1 - \frac{352944a_6}{7} \not\equiv 0 \pmod{7} \iff a_6 \not\equiv 14 \pmod{49}$$ since $$z \equiv z^7 \pmod{7}$$. This proves the proposition.

4.5 **The proof of Theorem 1**

We are now ready to derive Theorem 1 from our previous results.

Let $$E/\mathbb{Q}_p$$ and $$a_1, \ldots, a_6 \in p\mathbb{Z}_p$$ be as in the statement of the theorem. Then the Weierstrass curve

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$ over $$\mathbb{Z}_p$$ defines a minimal Weierstrass model of $$E$$. The theorem follows by applying to $$\mathcal{E}$$ part 2 of Proposition 11 if $$p > 7$$, or one of Propositions 13–18 if $$p \leq 7$$. 

12
5 Examples

In this section, we have collected some examples of elliptic curves over $\mathbb{Q}_p$ with additive reduction, such that their points of good reduction contains a $p$-torsion point. In particular, all curves and torsion points are defined over $\mathbb{Q}$. The fact that they possess a $p$-torsion point of good reduction can be verified using the appropriate result from the previous section. (Note that these result do not say when the $p$-torsion points will be defined over $\mathbb{Q}$.)

Example 19. 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.

Example 20. 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 21. 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 22. 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.

6 Acknowledgements

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

References

[1] Nikolay Nikolov and Dan Segal. On finitely generated profinite groups, I: strong completeness and uniform bounds. Ann. of Math., 165:171–238, 2007.

[2] J. Silverman. The Arithmetic of Elliptic Curves. Springer-Verlag, New York, 1986.

[3] Sir H.P.F. Swinnerton-Dyer. Density of rational points on certain surfaces. Unpublished, 2010.