Elliptic curves over Q_p

Winter, R.

Rosa Winter
rwinter@math.leidenuniv.nl

Elliptic curves over $\mathbb{Q}_p$

Bachelor thesis, August 23, 2011
Supervisor: Drs. R. Pannekoek

Mathematisch Instituut, Universiteit Leiden

Contents

Introduction

In this thesis we study elliptic curves over the field of p-adic numbers, denoted by $\mathbb{Q}_p$.

Diophantus of Alexandria lived between circa 200 and 298 AD and wrote a series of books called Arithmetica, in which he discussed solutions of algebraic equations. The study of these so-called Diophantine equations has been practiced ever since. Mathematicians are interested in both proving that integer or rational solutions of these equations exist and finding explicit solutions. Elliptic curves are examples of Diophantine equations of degree three. In studying them, we use techniques from algebraic geometry as well as from algebraic number theory. Much is already known about the set of rational points on elliptic curves. For example, this set can be made into an abelian group (Theorem 2.3.8). Furthermore, Mordell (1888-1972) proved that, in the case of an elliptic curve over the rational numbers, this group is finitely generated. There are also well known techniques to calculate the torsion points. Nonetheless, in practice it turns out that determining the isomorphism type of this group can be a hard task.

The study of p-adic numbers is more recent than elliptic curves. However, p-adic numbers play a central role in algebraic number theory. Kurt Hensel (1861-1941) first introduced them and he proved Hensel's Lemma (Lemma 1.2.9), which plays a very important role throughout this thesis. This lemma asserts that we can find solutions of certain polynomials over the p-adic integers, denoted by $\mathbb{Z}_p$, by looking for solutions in $\mathbb{F}_p$.

How do these two subjects, the study of elliptic curves and the study of p-adic numbers, relate? Helmut Hasse (1898-1979) proved that a second degree polynomial in two variables has rational solutions if it has solutions in $\mathbb{Q}_p$ for every prime p. Unfortunately, for elliptic curves this theorem does not hold, but we can still use the group of p-adic solutions of elliptic curves to understand the group of rational solutions. This is very useful, since the group of p-adic points on a curve is usually more easily found.

In this thesis we will explain how we can find the group of p-adic points on an elliptic curve. We will start the first chapter by defining the field of p-adic numbers and study some important and useful properties of both $\mathbb{Q}_p$ and $\mathbb{Z}_p$. We finish the chapter by stating and proving Hensel's Lemma. In the second chapter, we define the projective plane and elliptic curves. We explain how the group of points on an elliptic curve can be made into an abelian group. Finally, in the third chapter we will bring these two subjects together and study elliptic curves over $\mathbb{Q}_p$. We will finish the thesis by giving two explicit calculations of the group of p-adic points on an elliptic curve.

1 The p-adic numbers

In this chapter, we will define and explore the p-adic numbers. Recall that the real numbers $\mathbb{R}$ are constructed from $\mathbb{Q}$ by taking all Cauchy sequences in $\mathbb{Q}$ modulo all sequences that converge to zero. The p-adic numbers are constructed in a similar fashion, but instead of the standard norm we use the so-called p-adic norm.

1.1 The field $\mathbb{Q}_p$ and the ring $\mathbb{Z}_p$

We start this section by defining the notion of a *valuation* on a field K:

Definition 1.1.1. *Let K be a field. A map $\nu : K \longrightarrow \mathbb{R} \cup \infty$ is called a valuation if it satisfies the following properties for all $a, b \in K$:*

i. $\nu(ab) = \nu(a) + \nu(b)$;

ii. $\nu(a + b) \geq \min\{\nu(a), \nu(b)\}$ *with equality if* $\nu(a) \neq \nu(b)$;

iii. $\nu(a) = \infty \Leftrightarrow a = 0$.

We will focus on a specific valuation on the rational numbers, the *p-adic valuation.*

Definition 1.1.2. *Let p be a prime, and $a \in \mathbb{Q}^*$ a rational number. Write $a = p^\rho \cdot \frac{x}{y}$ with $x, y, \rho \in \mathbb{Z}$ and $p \nmid xy$. The p-adic valuation of a, denoted by $\nu_p(a)$, is defined as $\nu_p(a) = \rho$, with $\nu_p(0) = \infty$.*

Proposition 1.1.3. *ν_p is a valuation on $\mathbb{Q}$.*

Proof. Let $a, b \in \mathbb{Q}$. If a or b equals zero, properties *i* and *ii* are satisfied, since $\nu_p(0) = \infty$. If $a \neq 0 \neq b$, write $a = p^\rho \cdot \frac{x}{y}, b = p^\sigma \cdot \frac{x'}{y'}$ with $x, y, x', y', \rho, \sigma \in \mathbb{Z}$ and $p \nmid xy, p \nmid x'y'$. Then $\nu_p(ab) = \nu_p(p^{\rho+\sigma}\frac{xx'}{yy'}) = \rho + \sigma = \nu_p(a) + \nu_p(b)$, so ν_p satisfies property *i*. To prove property *ii*, write $a + b = \frac{p^\rho xy' + p^\sigma x'y}{yy'}$. Without loss of generality we may assume that $\rho \leq \sigma$, so that $a + b = p^\rho \frac{xy' + p^{\sigma-\rho}x'y}{yy'}$. We know that $p \nmid yy'$, therefore $\nu_p(a + b) \geq \rho = \min\{\nu_p(a), \nu_p(b)\}$. Note that if $\sigma \neq \rho$, the integer $xy' + p^{\sigma-\rho}x'y$ is not divisible by p, therefore $\nu_p(a + b) = \rho = \min\{\nu_p(a), \nu_p(b)\}$. Hence, ν_p satisfies property *ii* as well. Finally, property *iii* is satisfied by definition, so ν_p is a valuation on $\mathbb{Q}$. □

From the p-adic valuation we can construct the *p-adic norm* on $\mathbb{Q}$:

Definition 1.1.4. *Let p be a prime and $a \in \mathbb{Q}^*$. The p-adic norm of a, denoted by $|\cdot|_p$, is defined as $|a|_p = p^{-\nu_p(a)}$, with $|0|_p = 0$.*

Proposition 1.1.5. *$|\cdot|_p$ is a norm on $\mathbb{Q}$.*

Proof. Note that $|a|_p \geq 0$ for all $a \in \mathbb{Q}$, and $|a|_p = 0 \Leftrightarrow a = 0$ by definition. Now let $a, b \in \mathbb{Q}^*$. Then we have

$$|ab|_p = p^{-\nu_p(ab)} = p^{-\nu_p(a)-\nu_p(b)} = p^{-\nu_p(a)}p^{-\nu(b)} = |a|_p|b|_p$$

and $|a \cdot 0|_p = |0|_p = 0 = |a|_p|0|_p$, so $|\cdot|_p$ is multiplicative. Finally, we have

$$|a + b|_p = p^{-\nu_p(a+b)} \leq p^{-\min\{\nu_p(a),\nu_p(b)\}} = \max\{|a|_p, |b|_p\} \leq |a|_p + |b|_p$$

and $|a + 0|_p = |a|_p = |a|_p + |0|_p$, hence $|\cdot|_p$ satisfies the triangle inequality. We conclude that $|\cdot|_p$ is a norm on $\mathbb{Q}$. □

Since $|\cdot|_p$ is a norm, it satisfies the triangle inequality. In fact, we proved something stronger: for all $a, b \in \mathbb{Q}$ we have $|a+b|_p \leq \max\{|a|_p, |b|_p\}$. Norms that satisfy this property are called *ultrametric.* Furthermore, if $a, b \in \mathbb{Q}^*$ with $|a|_p \neq |b|_p$, we find $|a+b|_p = p^{-\nu_p(a+b)} = p^{-\min\{\nu_p(a), \nu_p(b)\}} = \max\{|a|_p, |b|_p\}$.

Note that $|\cdot|_p$ is a map from $\mathbb{Q}$ to $\mathbb{R}$ with image $\{p^n | n \in \mathbb{Z}\} \cup \{0\}$. With respect to the p-adic norm, numbers are small if they are divisible by high powers of p. We illustrate this by giving an example.

EXAMPLE 1.1.6. Consider the rational number $x = \frac{264}{245} = 2^3 \cdot 3 \cdot 5^{-1} \cdot 7^{-2} \cdot 11$. We calculate $|x|_p$ for different values of p:

$$|x|_2 = \frac{1}{8},\ |x|_3 = \frac{1}{3},\ |x|_5 = 5,\ |x|_7 = 49,\ |x|_{11} = \frac{1}{11}.$$

For all $p \notin \{2, 3, 5, 7, 11\}$, we have $|x|_p = 1$.

Since we defined a norm on $\mathbb{Q}$, we can talk about *Cauchy sequences* and *convergence* in $\mathbb{Q}$. For the convenience of the reader, we recall these two definitions.

DEFINITION 1.1.7. *Let k be a normed field with norm $|\cdot|$, and $(a_n)_{n\in\mathbb{N}}$ a sequence in k. We say that $(a_n)_{n\in\mathbb{N}}$ is a Cauchy sequence with respect to $|\cdot|$ if for all $\varepsilon > 0$ there exists an $N \in \mathbb{N}$ such that for all $m, n \geq N$ the equality $|a_n - a_m| < \varepsilon$ holds.*

DEFINITION 1.1.8. *Let k be a normed field with norm $|\cdot|$, and $(a_n)_{n\in\mathbb{N}}$ a sequence in k. The sequence $(a_n)_{n\in\mathbb{N}}$ is called convergent with respect to $|\cdot|$ if there exists an $a \in k$ with the property that for all $\varepsilon > 0$ there exists an $N \in \mathbb{N}$ such that for all $n \geq N$ the equality $|a_n - a| < \varepsilon$ holds. We say that $(a_n)_{n\in\mathbb{N}}$ converges to a, and we call a the limit of $(a_n)_{n\in\mathbb{N}}$.*

We are on our way to construct the field of p-adic numbers. Before we can do this, we need the following lemma:

LEMMA 1.1.9. *Let $(a_n)_{n\in\mathbb{N}}$ be a Cauchy sequence in $\mathbb{Q}$ that does not converge to zero with respect to $|\cdot|_p$. Then there exists an $N \in \mathbb{N}$ such that for all $n \geq N$ the equality $|a_n|_p = |a_N|_p \neq 0$ holds.*

Proof. Since $(a_n)_{n\in\mathbb{N}}$ does not converge to zero, there is an $\tilde{\varepsilon} > 0$ such that for all $N \in \mathbb{N}$ there exists an $n^* \geq N$ with $|a_{n^*}|_p \geq \tilde{\varepsilon}$. Now let $\varepsilon = \frac{\tilde{\varepsilon}}{2}$. Since $(a_n)_{n\in\mathbb{N}}$ is Cauchy, there exists an $N \in \mathbb{N}$ such that $|a_n - a_m|_p < \varepsilon$ for all $n, m \geq N$. Choose such an N, and choose n^* as above. Then by the triangle inequality we have

$$|a_N|_p \geq |a_{n^*}|_p - |a_{n^*} - a_N|_p > \tilde{\varepsilon} - \varepsilon = \varepsilon.$$

So for all $n \geq N$ we find $|a_N - a_n|_p < \varepsilon < |a_N|_p$. This means that $|a_N - a_n|_p \neq |a_N|_p$, so

$$|a_n|_p = |a_N - a_n - a_N|_p = \max\{|a_N - a_n|_p, |a_N|_p\} = |a_N|_p$$

for all $n \geq N$. Since $(a_n)_{n\in\mathbb{N}}$ does not converge to zero, and $|x|_p = 0 \Leftrightarrow x = 0$, it follows that $|a_N|_p \neq 0$. □

Now we have all the tools we need to construct the field of p-adic numbers. Let C be the set of Cauchy sequences in $\mathbb{Q}$. Note that C can be made into a ring by using component wise addition and multiplication. Let I be the set of sequences in C that converge to zero with respect to the p-adic norm. This is an ideal in C and, as we will now prove, it is even a maximal ideal.

Lemma 1.1.10. *I is a maximal ideal in C.*

Proof. Let J be another ideal of C such that $I \subsetneq J \subset C$. For $(a_n)_{n\in\mathbb{N}} \in J \setminus I$, only finitely many of the a_i are zero by Lemma 1.1.9, say $\{a_{i_1}, \ldots, a_{i_n}\}$. So the sequence $(b_n)_{n\in\mathbb{N}}$ given by $b_i = 1$ if $i \in \{i_1, \ldots, i_n\}$, $b_i = 0$ if $i \notin \{i_1, \ldots, i_n\}$ is an element of I, which means that $(c_n)_{n\in\mathbb{N}} = (a_n)_{n\in\mathbb{N}} + (b_n)_{n\in\mathbb{N}} \in J$, and $c_i \neq 0$ for all i. We want to prove that $(c_n^{-1})_{n\in\mathbb{N}} \in C$, which would mean that $(c_n)_{n\in\mathbb{N}} \cdot (c_n^{-1})_{n\in\mathbb{N}} = (1)_{n\in\mathbb{N}} \in J$, leading to $J = C$. To prove this, let $\varepsilon > 0$ be given. By Lemma 1.1.9 there exists an N such that $|c_n|_p = |c_N|_p \neq 0$ for all $n \geq N$. Choose $N' \geq N$ such that $|c_n - c_m|_p < \varepsilon |c_N|_p^2$ for all $n, m \geq N'$. Then for all $n, m \geq N'$:

$$|c_n^{-1} - c_m^{-1}|_p = \frac{|c_m - c_n|_p}{|c_n c_m|_p} = \frac{|c_m - c_n|_p}{|c_N|_p^2} < \frac{\varepsilon |c_N|_p^2}{|c_N|_p^2} = \varepsilon,$$

so $(c_n^{-1})_{n\in\mathbb{N}}$ is a Cauchy sequence. Hence, $(c_n^{-1})_{n\in\mathbb{N}} \in C$ and therefore $J = C$. We conclude that I is a maximal ideal in C. □

By the previous lemma, C/I is a field.

Definition 1.1.11. *The field of p-adic numbers is defined by $\mathbb{Q}_p = C/I$.*

The set of real numbers has certain properties, that make it a so-called *completion* of $\mathbb{Q}$ with respect to the standard norm. We will prove that $\mathbb{Q}_p$ has the same properties with respect to the p-adic norm. First we define what these properties are:

Definition 1.1.12. *Let K be a field and $k \subset K$ be a subfield, with norms $|\cdot|_K$ and $|\cdot|_k$ respectively. K is said to be the completion of k with respect to $|\cdot|_k$ if:*

i. *$|x|_K = |x|_k$ for all $x \in k$;*

ii. *K is complete with respect to $|\cdot|_K$;*

iii. *k is dense in K with respect to the topology induced by $|\cdot|_K$.*

To prove that $\mathbb{Q}_p$ is indeed a completion of $\mathbb{Q}$ with respect to the p-adic norm, we first show that $|\cdot|_p$ extends to a norm on $\mathbb{Q}_p$.

Definition 1.1.13. *Let x be an element in $\mathbb{Q}_p$ and $(a_n)_{n\in\mathbb{N}}$ a representative of x. The p-adic norm of x, denoted by $||x||_p$, is defined by $||x||_p = \lim_{n\to\infty} |a_n|_p$, with $||0||_p = 0$.*

Proposition 1.1.14. *$||\cdot||_p$ is well-defined and a norm on $\mathbb{Q}_p$.*

Proof. First, note that $||\cdot||_p$ exists, since by Lemma 1.1.9 the sequence $(|a_n|_p)_{n\in\mathbb{N}}$ will eventually be constant if it does not converge to zero, and for a sequence converging to zero the norm is zero by definition. Of course, we have to prove that $||\cdot||_p$ does not depend on the chosen representative of x. To this end, let $(b_n)_{n\in\mathbb{N}}$ be another representative of x. Then, by definition, $(a_n)_{n\in\mathbb{N}} - (b_n)_{n\in\mathbb{N}}$ is a Cauchy sequence converging to zero with respect to $|\cdot|_p$. Hence,

$$\begin{aligned}\lim_{n\to\infty} |a_n|_p = \lim_{n\to\infty} |a_n - b_n + b_n|_p \leq \lim_{n\to\infty} |a_n - b_n|_p + |b_n|_p \\ = \lim_{n\to\infty} |a_n - b_n|_p + \lim_{n\to\infty} |b_n|_p \\ = \lim_{n\to\infty} |b_n|_p,\end{aligned}$$

so $||x||_p$ is independent of the choice of representatives. What is left is to prove that $||\cdot||_p$ is indeed a norm. Since $|a|_p \geq 0$ for all $a \in \mathbb{Q}$, we have $||x||_p \geq 0$ for all $x \in \mathbb{Q}_p$. Furthermore, $||x||_p = 0 \Leftrightarrow x = 0$ by Lemma 1.1.9. To prove additivity and multiplicativity, let $x, y \in \mathbb{Q}_p^*$ (if x or y is zero it is trivial) and choose representatives $(a_n)_{n\in\mathbb{N}}, (b_n)_{n\in\mathbb{N}}$, respectively. Then

$$||xy||_p = \lim_{n\to\infty} |a_n b_n|_p = \lim_{n\to\infty} |a_n|_p |b_n|_p = \lim_{n\to\infty} |a_n|_p \lim_{n\to\infty} |b_n|_p = ||x||_p ||y||_p,$$

and

$$\begin{aligned}||x+y||_p = \lim_{n\to\infty} |a_n + b_n|_p \leq \lim_{n\to\infty} \max\{|a_n|_p, |b_n|_p\} \leq \lim_{n\to\infty} |a_n|_p + \lim_{n\to\infty} |b_n|_p \\ = ||x||_p + ||y||_p,\end{aligned}$$

so $||\cdot||_p$ is a norm. In fact, the above shows that $||x+y||_p \leq \max\{||x||_p, ||y||_p\}$ for all $x, y \in \mathbb{Q}$, so $||\cdot||_p$ is an ultrametric norm. □

Now that we have a well-defined norm on $\mathbb{Q}_p$, we can prove that $\mathbb{Q}_p$ is the completion of $\mathbb{Q}$ with respect to the p-adic norm.

Proposition 1.1.15. *$\mathbb{Q}_p$, with norm $||\cdot||_p$, is a completion of $\mathbb{Q}$ with respect to the p-adic norm.*

Proof. Consider the canonical homomorphism $i : \mathbb{Q} \hookrightarrow \mathbb{Q}_p$, $q \longmapsto \overline{(q,q,q,\dots)}$ (where $\overline{(q,q,q,\dots)}$ is the class of the constant sequence $(q,q,q,\dots)$ in $\mathbb{Q}_p$). Note that $||i(q)||_p = |q|_p$ for all $q \in \mathbb{Q}$. To prove that $\mathbb{Q}$ is dense in $\mathbb{Q}_p$, let x be an element in $\mathbb{Q}_p$ and $\varepsilon > 0$. We will show that there exists an element $y \in \mathbb{Q}$ such that $||x - i(y)||_p < \varepsilon$. Let $(a_n)_{n\in\mathbb{N}}$ be a representative of x. Since $(a_n)_{n\in\mathbb{N}}$ is a Cauchy sequence with respect to $|\cdot|_p$, there exists an N such that $|a_n - a_m|_p < \varepsilon$ for all $n, m \geq N$. Let $y = a_N$. Then

$$||x - i(y)||_p = \lim_{n\to\infty} |a_n - y|_p = \lim_{n\to\infty} |a_n - a_N|_p < \varepsilon,$$

so $\mathbb{Q}$ is dense in $\mathbb{Q}_p$. The last thing to prove is that $\mathbb{Q}_p$ is complete with respect to the norm $||\cdot||_p$. Let $(x_n)_{n\in\mathbb{N}}$ be a Cauchy sequence in $\mathbb{Q}_p$. We will prove that $(x_n)_{n\in\mathbb{N}}$ converges to a limit in $\mathbb{Q}_p$. Since $\mathbb{Q}$ is dense in $\mathbb{Q}_p$, for every $n \in \mathbb{N}$ there exists an $y_n \in \mathbb{Q}$ such that $||x_n - i(y_n)||_p < \frac{1}{n}$. We will show that the sequence $(y_n)_{n\in\mathbb{N}}$ is a Cauchy sequence in $\mathbb{Q}$. To this end, let $\varepsilon > 0$, and $N \in \mathbb{N}$ such that $N \geq \frac{1}{\varepsilon}$. Then for all $n \geq N$ we find $||x_n - i(y_n)||_p < \frac{1}{n} \leq \frac{1}{N} \leq \varepsilon$. So $(x_n - i(y_n))_{n\in\mathbb{N}}$ converges to zero, from which it follows that it is a Cauchy sequence. Hence $(i(y)_n)_{n\in\mathbb{N}} = (x_n)_{n\in\mathbb{N}} - (x_n - i(y_n))_{n\in\mathbb{N}}$ is a Cauchy sequence in $\mathbb{Q}_p$ too. But $||i(y_n)||_p = |y_n|_p$ for all $n \in \mathbb{N}$, so $(y_n)_{n\in\mathbb{N}}$ is a Cauchy sequence in $\mathbb{Q}$ with respect to

$| \cdot |_p$. Hence, $x = \overline{(y_n)_{n\in\mathbb{N}}}$ is an element in $\mathbb{Q}_p$. Next, we want to prove that x is the limit of $(x_n)_{n\in\mathbb{N}}$ in $\mathbb{Q}_p$. We start by proving that $(x - i(y_n))_{n\in\mathbb{N}}$ converges to zero. Let $\varepsilon > 0$, and choose N such that $|y_n - y_m|_p < \varepsilon$ for all $n, m \geq N$. Then for all $n \geq N$, we find $||x - i(y_n)||_p = \lim_{m\to\infty} |y_m - y_n|_p < \varepsilon$. So $(x - i(y_n))_{n\in\mathbb{N}}$ converges to zero, hence $(x - x_n)_{n\in\mathbb{N}} = (x - i(y_n))_{n\in\mathbb{N}} - (x_n - i(y_n))_{n\in\mathbb{N}}$ converges to zero. We conclude that $(x_n)_{n\in\mathbb{N}}$ converges to x in $\mathbb{Q}_p$, so $\mathbb{Q}_p$ is complete with respect to $|| \cdot ||_p$. □

Since $\mathbb{Q}$ is dense in $\mathbb{Q}_p$, for all $x \in \mathbb{Q}_p$ there is an $y \in \mathbb{Q}$ with $||x - i(y)||_p < ||i(y)||_p$, so $||x||_p = ||x - y + y||_p = ||i(y)||_p = |y|_p$. We conclude that the image of the map $|| \cdot ||_p$ on $\mathbb{Q}_p$ is exactly the same as the the image of $| \cdot |_p$. From now on, for an element $q \in \mathbb{Q}$ we write $q = \overline{(q, q, q, \ldots)} \in \mathbb{Q}_p$. Furthermore, for an element $x \in \mathbb{Q}_p$ we will write $|x|_p$ instead of $||x||_p$.

Definition 1.1.16. *The set $\mathbb{Z}_p = \{x \in \mathbb{Q}_p : |x|_p \leq 1\}$ is called the set of p-adic integers.*

Proposition 1.1.17. *$\mathbb{Z}_p$ is a subring of $\mathbb{Q}_p$.*

Proof. Clearly, $1 = (1, 1, 1, \ldots)$ and $0 = (0, 0, 0, \ldots)$ are in $\mathbb{Z}_p$. Let $x, y \in \mathbb{Z}_p$, then $|x|_p \leq 1$, $|y|_p \leq 1$. This implies

$$|x + y|_p \leq \max\{|x|_p, |y|_p\} \leq 1 \text{ and } |xy|_p = |x|_p|y|_p \leq 1,$$

so $\mathbb{Z}_p$ is closed under addition and multiplication. Finally, $| - x|_p = |x|_p \leq 1$, so $-x \in \mathbb{Z}_p$. This implies that $\mathbb{Z}_p$ is a subring of $\mathbb{Q}_p$. □

We will describe and understand the ring $\mathbb{Z}_p$ thoroughly in this thesis. As we will see later, $\mathbb{Z}_p$ has the following property which states that we can very easily find solutions of polynomials in $\mathbb{Z}_p[x]$.

Theorem 1.1.18. *Let $f \in \mathbb{Z}_p[x]$ be a polynomial and assume that there is an $a \in \mathbb{Z}_p$ with $f(a) \in p\mathbb{Z}_p$ and $f'(a) \in \mathbb{Z}_p^*$. Then there exists a $b \in \mathbb{Z}_p$ with $b \equiv a$ mod p and $f(b) = 0$.*

Proof. This is a special case of Hensel's lemma, which is our main result in Section 1.2. □

Definition 1.1.19. *An element $x \in \mathbb{Q}_p$ with $|x|_p = 1$ is called a p-adic unit.*

For a p-adic unit u we have $|u^{-1}|_p = |u|_p^{-1} = 1$, so $u^{-1} \in \mathbb{Z}_p$ is a p-adic unit too. Furthermore, if x is an invertible element of $\mathbb{Z}_p$, then $|x|_p \leq 1$ and $|x^{-1}|_p = |x|_p^{-1} \leq 1$, so $|x|_p = |x^{-1}|_p = 1$, which means that x is a p-adic unit. We conclude that the p-adic units are exactly the invertible elements of $\mathbb{Z}_p$. Furthermore, from what is said about the image of $|| \cdot ||_p$ it follows that every element in $\mathbb{Q}_p^*$ is of the form $p^n u$, with $n \in \mathbb{Z}$ and u a p-adic unit.

Definition 1.1.20. *A ring is called a discrete valuation ring if it is a Noetherian, local ring and its maximal ideal is generated by an element that is not nilpotent.*

Proposition 1.1.21. *$\mathbb{Z}_p$ is a discrete valuation ring.*

Proof. We know that a ring R is a local if $R \setminus R^*$ is an ideal. Furthermore, we showed that $\mathbb{Z}_p^* = \{x \in \mathbb{Q}_p | |x|_p = 1\}$. Note that $0 \in \mathbb{Z}_p \setminus \mathbb{Z}_p^*$, since $|0|_p = 0 < 1$. For $x, x' \in \mathbb{Z}_p \setminus \mathbb{Z}_p^*$ we have $|x|_p < 1$ and $|x'|_p < 1$, so $|x + x'|_p \leq \max\{|x|_p, |x'|_p\} < 1$ and $|-x|_p = |x|_p < 1$. Hence, $x + x' \in \mathbb{Z}_p \setminus \mathbb{Z}_p^*$, $-x \in \mathbb{Z}_p \setminus \mathbb{Z}_p^*$. Finally, let $y \in \mathbb{Z}_p$, then $|xy|_p = |x|_p|y|_p < 1$, so $xy \in \mathbb{Z}_p \setminus \mathbb{Z}_p^*$. We conclude that $\mathbb{Z}_p \setminus \mathbb{Z}_p^*$ is an ideal, and $\mathbb{Z}_p$ is a local ring with maximal ideal $\mathbb{Z}_p \setminus \mathbb{Z}_p^*$. What is left to prove is that $\mathbb{Z}_p \setminus \mathbb{Z}_p^*$ is generated by an element that is not nilpotent. To prove this, first note that for an element x in $\mathbb{Z}_p \setminus \mathbb{Z}_p^*$ we have $|p^{-1}x|_p \leq 1$, so $x \in p\mathbb{Z}_p$. Furthermore, an element y in $p\mathbb{Z}_p$ is of the form $y = p^n u$, with $n \in \mathbb{Z}_{>0}$, so $|y|_p < 1$, which means that $y \in \mathbb{Z}_p \setminus \mathbb{Z}_p^*$. We find $\mathbb{Z}_p \setminus \mathbb{Z}_p^* = p\mathbb{Z}_p$. This ideal is generated by p, which is not a nilpotent element. We conclude that $\mathbb{Z}_p$ is a discrete valuation ring. □

The previous proposition tells us a lot about the structure of $\mathbb{Z}_p$. With help of the following two lemmas, we can understand $\mathbb{Z}_p$ even better. That is, we can give an explicit description of the elements in $\mathbb{Z}_p$.

Definition 1.1.22. *For all $n \in \mathbb{N}$, let x_n be an element of $\mathbb{Q}$. We denote the sequence $(\sum_{n=0}^{N} x_n p^n)_{N \in \mathbb{N}}$ by $\sum_{n=0}^{\infty} x_n p^n$.*

Lemma 1.1.23. *If $x_n \in \{0, \dots, p-1\}$ for all n, then $(\sum_{n=0}^{N} x_n p^n)_{N \in \mathbb{N}}$ is a Cauchy sequence with respect to the p-adic norm.*

Proof. Let $\varepsilon > 0$, and choose N such that $p^{-N} < \varepsilon$. Then for all $m \geq l \geq N$ we have

$$\left| \sum_{n=0}^{m} x_n p^n - \sum_{n=0}^{l} x_n p^n \right|_p = \left| \sum_{n=l+1}^{m} x_n p^n \right|_p \leq \max_{l<n\leq m} \{|x_n p^n|_p\} < p^{-l} < \varepsilon.$$

So the sequence $(\sum_{n=0}^{N} x_n p^n)_{N \in \mathbb{N}}$ is a Cauchy sequence with respect to the p-adic norm. □

Lemma 1.1.24. *For all $x \in \mathbb{Z}_p$, $m \in \mathbb{N}$ there exist unique $x_0, \dots, x_m \in \{0, \dots, p-1\}$ such that $|x - \sum_{n=0}^{m} x_n p^n|_p < p^{-m}$, where the x_n do not depend on m.*

Proof. Uniqueness is easily checked, so we will prove existence. Let $x \in \mathbb{Q}_p$. Since $\mathbb{Q}$ is dense in $\mathbb{Q}_p$, there is a $y \in \mathbb{Q}$ with $|x - y|_p < 1$. From $|y|_p \leq \max\{|x|_p, |y - x|_p\} \leq 1$ it follows that $y \in \mathbb{Z}_p$. Hence, y is of the form $\frac{a}{b}$ with $\alpha, \beta \in \mathbb{Z}$ and $p \nmid \beta$. This means that $\gcd(p, b) = 1$, so there is a $b' \in \mathbb{Z}$ such that $bb' \equiv 1 \bmod p$. Let $x_0 \equiv ab' \bmod p$, then

$$|y - x_0|_p = \left| \frac{a}{b}(1 - b'b) + kp \right|_p \leq \max\{|y|_p |1 - bb'|_p, |kp|_p\} < 1$$

for a certain $k \in \mathbb{Z}$. It follows that

$$|x - x_0|_p = |x - y + y - x_0|_p \leq \max\{|x - y|_p, |y - x_0|_p\} < 1,$$

so for $m = 0$ this lemma is true.
Now assume that this lemma is true for all $m \leq N$. Then there exist unique $x_0, \dots, x_N \in \{0, \dots, p-1\}$ with $|x - \sum_{n=0}^{N} x_n p^n|_p < p^{-N}$. Let $z = x - \sum_{n=0}^{N} x_n p^n$,

then $|p^{-N-1}z| \leq 1$ so by the induction hypothesis there is a unique $\tilde{z} \in \{0, \ldots, p-1\}$ with $|p^{-N-1}z - \tilde{z}|_p < 1$, hence $|z - p^{N+1}\tilde{z}|_p < p^{-N-1}$. Set $x_{N+1} = \tilde{z}$, then

$$\left|x - \sum_{n=0}^{N+1} x_n p^n\right|_p = \left|x - \sum_{n=0}^{N} x_n p^n - \tilde{z}p^{N+1}\right|_p = \left|z - p^{N+1}\tilde{z}\right|_p < p^{-(N+1)}.$$

From the construction of the x_n it is clear that they do not depend on m. We conclude that the lemma holds for all m. □

We are now able to give an explicit description of the elements of $\mathbb{Z}_p$.

Proposition 1.1.25. *The elements in $\mathbb{Z}_p$ are exactly the elements of the form*

$$x = \sum_{n=0}^{\infty} x_n p^n,$$

with $x_n \in \{0, \ldots, p-1\}$.

Proof. Consider the sequence $\sum_{n=0}^{\infty} x_n p^n$ with $x_n \in \{0, \ldots, p-1\}$. It is a sequence in $\mathbb{Z}_p$ and it converges to an element in $\mathbb{Q}_p$ by Lemma 1.1.23. Since $\mathbb{Z}_p$ is a closed subset of $\mathbb{Q}_p$, the sequence converges to an element in $\mathbb{Z}_p$, so $\sum_{n=0}^{\infty} x_n p^n \in \mathbb{Z}_p$. Now let $x \in \mathbb{Z}_p$. It follows immediately from Lemma 1.1.24 that for all $m \in \mathbb{N}$ there are unique $x_0, \ldots, x_m \in \{0, \ldots, p-1\}$ such that $x - (\sum_{n=0}^{N} x_n p^n)_{N\in\mathbb{N}}$ converges to zero. We conclude that $x = (\sum_{n=0}^{N} x_n p^n)_{N\in\mathbb{N}} = \sum_{n=0}^{\infty} x_n p^n$. □

From the previous proposition, we see that every element x in $\mathbb{Z}_p$ is uniquely represented by a Cauchy sequence of the form $(x_0, x_0 + x_1 p, x_0 + x_1 p + x_2 p^2, \ldots)$, where $x_i \in \{0, \ldots, p-1\}$ for all i. We call this Cauchy sequence the *standard representative* of x.

Writing every element in $\mathbb{Z}_p$ as an infinite series in powers of p, we don't add two elements like we add usual power series in one variable. Two series in $\mathbb{Z}_p$ are added by so called 'carrying'. Consider the sequence $a = \sum_{n=0}^{\infty} a_n p^n$ with $a_n \in \mathbb{N}$. Define $k_0 = 0$, $k_i = \nu_p(a_{i-1} + k_{i-1})$. Then we construct $a' = \sum_{n=0}^{\infty} a'_n p^n$ from a through carrying by setting $a'_i = (a_i + k_i) - k_{i+1}p$. Note that $a'_i \in \{0, \ldots, p-1\}$ for all i, hence a' is an element in $\mathbb{Z}_p$. We illustrate the concept of carrying by an example:

Example 1.1.26. Let $a = 2 + 1 \cdot 3 + 0 \cdot 3^2 + \ldots$, $b = 2 + 1 \cdot 3 + 1 \cdot 3^2 + \ldots$ be two elements of $\mathbb{Z}_3$, then their sum is given by

$$a + b = 1 + 0 \cdot 3 + 2 \cdot 3^2 + \ldots$$

Lemma 1.1.27. *Let*

$$a = (a_0, a_0 + a_1 p, a_0 + a_1 p + a_2 p^2, \ldots),\ a' = (a'_0, a'_0 + a'_1 p, a'_0 + a'_1 p + a'_2 p^2, \ldots)$$

be two Cauchy sequences in $\mathbb{Q}$ converging to the same element. Then

$$\sum_{n=0}^{m} a_n p^n \equiv \sum_{n=0}^{m} a'_n p^n \ \mathit{mod}\ p^{m+1}$$

for all $m \in \mathbb{N}$.

Proof. Since a and a' converge to the same element, their difference $a - a'$ converges to zero. So $\sum_{n=0}^{\infty}(a_n - a'_n)p^n = 0$, which means that

$$\sum_{n=0}^{m}(a_n - a'_n)p^n = -\sum_{n=m+1}^{\infty}(a_n - a'_n)p^n \equiv 0 \bmod p^{m+1}$$

for all $m \in \mathbb{N}$. □

We finish this section by the following proposition, which we will use later.

PROPOSITION 1.1.28. *Let p be a prime. There exists a canonical isomorphism*

$$\psi : \mathbb{Z}_p/p\mathbb{Z}_p \longrightarrow \mathbb{Z}/p\mathbb{Z}.$$

Proof. Consider the projection

$$\pi : \mathbb{Z}_p \longrightarrow \mathbb{Z}/p\mathbb{Z}, \sum_{n=0}^{\infty} a_n p^n \longmapsto a_0.$$

First note that $\pi(1) = \pi(1 + 0 \cdot p + 0 \cdot p^2 + \ldots) = 1$. Furthermore, for $a, b \in \mathbb{Z}_p$ we have $\pi(a+b) = \pi(a) + \pi(b)$ and $\pi(ab) = \pi(a)\pi(b)$ by Lemma 1.1.27, so π is a ring homomorphism. We claim that the kernel is exactly the ideal $p\mathbb{Z}_p \subset \mathbb{Z}_p$. To prove one implication, let $a = \sum_{n=0}^{\infty} a_n p^n$ be an element of $p\mathbb{Z}_p$. Then $a_0 = 0$, so $\pi(a) = a_0 = 0$, which means that a is in the kernel of π. Now let $a = \sum_{n=0}^{\infty} a_n p^n$ be an element in the kernel of π. Then $a_0 = 0$, so $p|a$, hence $a \in p\mathbb{Z}_p$. We conclude that the kernel of π is the ideal $p\mathbb{Z}_p$, so

$$\mathbb{Z}_p/p\mathbb{Z}_p \cong \pi(\mathbb{Z}_p) = \mathbb{Z}/p\mathbb{Z}.$$

□

1.2 Hensel's Lemma

Hensel's lemma states that, under certain conditions, we can quite easily find solutions of polynomials in $\mathbb{Z}_p$. Before we can state and prove Hensel's lemma, we have to define what it means for a ring R to be complete with respect to an ideal $I \subset R$. This definition has to do with the *projective limit* of R with respect to I.

DEFINITION 1.2.1. *Let R be a ring, and $I \subset R$ an ideal. The projective limit of R with respect to I is the subring of $\prod_{n \in \mathbb{Z}_{\geq 1}} R/I^n$ given by*

$$\varprojlim_n R/I^n = \left\{ (a_1, a_2, a_3 \ldots) \in \prod_{n \in \mathbb{Z}_{\geq 1}} R/I^n | a_m \equiv a_n \text{ mod } I^n \text{ for all } n \leq m \right\}.$$

We denote the projective limit by $\hat{R}_I$.

To verify that $\hat{R}_I$ is indeed a subring of $\prod_{n \in \mathbb{Z}_{\geq 1}} R/I^n$, note that the sum of two elements in $\hat{R}_I$ is again an element of $\hat{R}_I$, and the product too. Furthermore,

$(0,0,0,\ldots) \in \hat{R}_I$ and $(1,1,1,\ldots) \in \hat{R}_I$. Finally, for an element in $\hat{R}_I$ the additive inverse is in $\hat{R}_I$, too, so $\hat{R}_I$ is indeed a subring of $\prod_{n\in\mathbb{Z}_{\geq 1}} R/I^n$. There exists a ringhomomorphism

$$\varphi : R \longrightarrow \hat{R}_I \text{ }, r \mapsto (r \bmod I, r \bmod I^2, r \bmod I^3, \ldots).$$

For $r \in R$, we will denote $\varphi(r)$ by r.

Example 1.2.2. Let $R = \mathbb{Z}$, and for p prime let $I = (p)$. The projective limit of $\mathbb{Z}$ with respect to (p) is the ring

$$\hat{\mathbb{Z}}_{(p)} = \{(a_1, a_2, ...) \in \prod_{n\in\mathbb{N}} \mathbb{Z}/p^n\mathbb{Z} | a_m \equiv a_n \bmod p^n, n \leq m\}.$$

Proposition 1.2.3. *There exists an isomorphism* $\psi : \mathbb{Z}_p \longrightarrow \hat{\mathbb{Z}}_{(p)}$.

Proof. By Proposition 1.1.25, every element $x \in \mathbb{Z}_p$ is of the form $\sum_{n=0}^{\infty} x_n p^n$ for certain $x_n \in \{0, \ldots, p-1\}$. Consider the map

$$\psi : \mathbb{Z}_p \longrightarrow \hat{\mathbb{Z}}_{(p)},$$

$$\sum_{n=0}^{\infty} x_n p^n \longmapsto (x_0 \bmod p, (x_0 + x_1 p) \bmod p^2, (x_0 + x_1 \cdot p + x_2 \cdot p^2) \bmod p^3, \ldots).$$

Note that for all $x \in \mathbb{Z}$ the element $\psi(x)$ is indeed an element of $\hat{\mathbb{Z}}_{(p)}$, so the map is well-defined. To ease notation, for an element $\sum_{n=0}^{\infty} x_n p^n$ in $\mathbb{Z}_p$ we will write

$$\psi\left(\sum_{n=0}^{\infty} x_n p^n\right) = (x_0, x_0 + x_1 p, x_0 + x_1 \cdot p + x_2 \cdot p^2, \ldots),$$

where $\sum_{n=0}^{N} x_n p^n$ is interpreted as an element of $\in \mathbb{Z}/p^{N+1}\mathbb{Z}$. We will prove that ψ is a ring isomorphism. Note that the unit element $1 = 1 + 0 \cdot p + 0 \cdot p^2 + 0 \cdot p^3 + \ldots$ is mapped to $(1,1,1,\ldots)$. Now let $a = \sum_{n=0}^{\infty} a_n p^n$, $b = \sum_{n=0}^{\infty} b_n p^n$ be two standard representatives of elements in $\mathbb{Z}_p$, with $c = \sum_{n=0}^{\infty} c_n p^n$ their sum constructed by carrying. Then:

$$\begin{aligned}
\psi(a) + \psi(b) &= (a_0 + b_0, a_0 + b_0 + (a_1 + b_1)p, a_0 + b_0 + (a_1 + b_1)p + (a_2 + b_2)p^2, \ldots) \\
&= (c_0, c_0 + c_1 p, c_0 + c_1 p + c_2 p^2, \ldots) \text{ (Lemma 1.1.27)} \\
&= \psi(c) = \psi(a + b),
\end{aligned}$$

so $\psi(a+b) = \psi(a) + \psi(b)$ for all $a, b \in \mathbb{Z}_p$. Our next step is to prove multiplicativity. Write $ab = \sum_{n=0}^{\infty}(\sum_{k=0}^{n} a_k b_{n-k}) p^n = \sum_{n=0}^{\infty} d_n p^n$, where the latter is constructed by carrying. Then:

$$\begin{aligned}
\psi(a)\psi(b) &= \left(\sum_{n=0}^{0}\left(\sum_{k=0}^{n} a_k b_{n-k}\right) p^n, \sum_{n=0}^{1}\left(\sum_{k=0}^{n} a_k b_{n-k}\right) p^n, \sum_{n=0}^{2}\left(\sum_{k=0}^{n} a_k b_{n-k}\right) p^n, \ldots\right) \\
&= (d_0, d_0 + d_1 p, d_0 + d_1 p + d_2 p^2, \ldots) \text{ (Lemma 1.1.27)} \\
&= \psi(ab),
\end{aligned}$$

hence $\psi(ab) = \psi(a)\psi(b)$ for all $a, b \in \mathbb{Z}_p$.
We now proved that ψ is a ring homomorphism, which leaves us to show that ψ is bijective. We start by proving injectivity. Let $x = \sum_{n=0}^{\infty} x_n p^n \in \mathbb{Z}_p$ with $\psi(x) = 0$. Then $x \in p^n\mathbb{Z}$ for all n, from which it follows that $x = 0$, so ψ is injective. To prove surjectivity, let $(\overline{a}_1, \overline{a}_2, \overline{a}_3, \ldots)$ be an element in $\hat{\mathbb{Z}}_{(p)}$ and a_i a representative of $\overline{a}_i$ in $\mathbb{Z}$ for each i. We will show by induction that for every $n \in \mathbb{N}$ there exist $\alpha_0, \ldots, \alpha_n$, with $\alpha_i \in \{0, \ldots, p-1\}$ for all $0 \leq i \leq n$, such that $\sum_{i=0}^{n} \alpha_i p^i \equiv a_{n+1} \bmod p^{n+1}$ and where the α_i do not depend on n. For $n = 0$, let $\alpha_0 \equiv a_1 \bmod p$. Now assume that our claim holds for all $n < N$. Then there exist $\alpha_0, \ldots, \alpha_{N-1}$ with $\alpha_i \in \{0, \ldots, p-1\}$ such that $\sum_{i=0}^{N-1} \alpha_i p^i \equiv a_N \bmod p^N$. By the property of the projective limit we have

$$\sum_{i=0}^{N-1} \alpha_i p^i \equiv a_N \equiv a_{N+1} \bmod p^N,$$

so there is an $\alpha_N \in \{0, \ldots, p-1\}$ such that

$$\sum_{i=0}^{N-1} \alpha_i p^i + \alpha_N p^N \equiv a_{N+1} \bmod p^{N+1}.$$

It follows that our claim holds for all n and from the construction of the α_i it is clear that they do not depend on n. Furthermore, $\alpha_i \in \{0, \ldots, p-1\}$ for all i, so $\sum_{n=0}^{\infty} \alpha_n p^n \in \mathbb{Z}_p$. We find $\psi\left(\sum_{n=0}^{\infty} \alpha_n p^n\right) = (a_1, a_2, a_3, \ldots)$, hence ψ is surjective. □

Proposition 1.2.3 is a very useful proposition, since it tells us that we can identify $\mathbb{Z}_p$ with both the ring of p-adic integers and the projective limit of $\mathbb{Z}$ with respect to the ideal (p). We can often use this to prove things about $\mathbb{Z}_p$ that seem difficult using one definition, by switching to the other.

Definition 1.2.4. *A ring R is complete with respect to an ideal I if $\varphi : R \longrightarrow \hat{R}_I$, $r \mapsto (r \bmod I, r \bmod I^2, r \bmod I^3, \ldots)$ is an isomorphism.*

Definition 1.2.5. *Let R be a complete ring. A sequence $(x_n)_{n\in\mathbb{N}}$ of elements in R is said to converge to a limit x in R if for all $N \in \mathbb{N}$ there exists an M such that for all $m \geq M$ the equality $x_m - x \in I^N$ holds.*

Example 1.2.6. Let R be a ring, and $I = (0)$. Then

$$\hat{R}_I = \{(a_1, a_2, a_3, \ldots) \in \prod_{n\in\mathbb{Z}_{\geq 1}} R | a_1 \equiv a_2 \equiv a_3 \equiv \ldots \bmod 0\}.$$

Note that the condition in the description says that $a_1 = a_2 = a_3 = \ldots$, so $\hat{R}_I$ consists exactly of all constant sequences of elements in R, which means that φ is an isomorphism. Hence, every ring is complete with respect to its zero ideal.

Example 1.2.7. Consider the ring $\hat{\mathbb{Z}}_{(p)}$, and the ideal $(p) = p\hat{\mathbb{Z}}_{(p)} \subset \hat{\mathbb{Z}}_{(p)}$. We will prove that $\hat{\mathbb{Z}}_{(p)}$ is complete with respect to (p). By Proposition 1.2.3, we know that

$\hat{\mathbb{Z}}_{(p)}$ is isomorphic to $\mathbb{Z}_p$. This means that proving that $\hat{\mathbb{Z}}_{(p)}$ is complete with respect to (p) is equivalent to proving that the homomorphism

$$\varphi : \mathbb{Z}_p \longrightarrow \varprojlim_n \mathbb{Z}_p/p^n\mathbb{Z}_p,$$

$$\sum_{n=0}^{\infty} x_n p^n \mapsto \left(\sum_{n=0}^{\infty} x_n p^n \bmod p, \sum_{n=0}^{\infty} x_n p^n \bmod p^2, \sum_{n=0}^{\infty} x_n p^n \bmod p^3, \ldots \right)$$

is bijective. Let $x = \sum_{n=0}^{\infty} x_n p^n \in \mathbb{Z}_p$ with $\varphi(x) = 0$. Then $x \in p^n\mathbb{Z}_p$ for all $n \in \mathbb{N}$, which leads to $x = 0$, so φ is injective. To prove surjectivity, let $(\overline{a}_1, \overline{a}_2, \overline{a}_3, \ldots)$ be an element of $\varprojlim_n \mathbb{Z}_p/p^n\mathbb{Z}_p$. For all i, choose the representative of $\overline{a}_i$ given by $a_i = \sum_{n=0}^{i-1} a_{in} p^n$, where $a_{ij} \in \{0, \ldots, p-1\}$, in $\mathbb{Z}_p$. Then a_{ij} is uniquely determined for all $i \in \mathbb{Z}_{\geq 1}$, $1 \leq j \leq i-1$. Moreover, by the property of the projective limit, $a_j \equiv a_i \bmod p^i$ for all $j \geq i$, so $\sum_{n=0}^{j} a_{jn} p^n \equiv \sum_{n=0}^{i-1} a_{in} p^n \bmod p^i$ for all $j \geq i$. We can now choose m big enough such that $\varphi(a_m) = (\overline{a}_1, \overline{a}_2, \overline{a}_3, \ldots)$, so φ is surjective.

Definition 1.2.8. *Let R be a complete ring, and $x_n \in R$ for all $n \in \mathbb{N}$. We denote the sequence $(\sum_{n=0}^{N} x_n)_{N \in \mathbb{N}}$ in R by $\sum_{n=0}^{\infty} x_n$. If this sequence converges to x, we write*

$$x = \sum_{n=0}^{\infty} x_n.$$

Lemma 1.2.9 (Hensel). *Let R be a ring that is complete with respect to an ideal $I \subset R$, and let $f(x) \in R[x]$ a polynomial. Assume that there exists an $n \geq 1$ and an $a \in R$ such that $f(a) \in I^n$ and $f'(a) \in R^*$. Then, for all $\alpha \in R$ with $\alpha \equiv f'(a)$ mod I, the sequence given by*

$$\omega_0 = a,\ \omega_{m+1} = \omega_m - \frac{f(\omega_m)}{\alpha}$$

converges to an element $b \in R$ with $b \equiv a$ mod I and $f(b) = 0$.

Proof. First, for $\frac{f(\omega_m)}{\alpha}$ to make sense, we show that $\alpha \in R^*$. Since $\alpha \equiv f'(a) \bmod I$, α is of the form $f'(a) + i$ with $i \in I$. Note that $f'(a) \in R^*$, so $\beta = (f'(a))^{-1}$ exists. But then

$$\alpha \sum_{n=0}^{\infty} \beta(-\beta i)^n = \sum_{n=0}^{\infty} (1 + \beta i)(-\beta i)^n = \sum_{n=0}^{\infty} (-\beta i)^n + (-1)^n(\beta i)^{n+1} = 1,$$

so $\alpha \in R^*$.

Now write $\omega = v + a$ and $g(v) = \frac{f(v+a)}{\alpha}$, then we know that $g(0) = \frac{f(a)}{\alpha} \in I^n$, $g'(0) = f'(a) \equiv 1 \bmod I$. We need to prove that the sequence

$$v_0 = 0,\ v_{m+1} = v_m - g(v_m)$$

converges to an element b with $g(b) = 0$ and $b \equiv 0 \bmod I^n$.

To this end, first note that since $g(0) \in I^n$ we have $v_m \in I^n \Rightarrow v_m - g(v_m) \in I^n$. Since $v_0 = 0 \in I^n$, we find

$$v_m \in I^n \text{ for all } m \geq 0. \tag{1}$$

To continue the proof, we will need the following lemma:

LEMMA 1.2.10. $v_{m+1} - v_m \in I^{m+n}$ *for all* $m \in \mathbb{N}$.

Proof. We prove this with induction. For $m = 0$, we have $v_1 - v_0 = v_1 = -g(0) \in I^n$. Now assume that $v_{m+1} - v_m \in I^{m+n}$ for all $m < M$. We calculate $v_{M+1} - v_M$. Write $g(v) = \sum_{i=0}^d a_i v^i$ (where d is the degree of g), then we find:

$$\begin{aligned}
v_{M+1} - v_M &= v_M - g(v_M) - v_{M-1} + g(v_{M-1}) \\
&= v_M - v_{M-1} - (g(v_M) - g(v_{M-1})) \\
&= v_M - v_{M-1} - \sum_{i=0}^{d} a_i (v_M^i - v_{M-1}^i) \\
&= v_M - v_{M-1} - g'(0)(v_M - v_{M-1}) - \sum_{i=2}^{d} a_i (v_M^i - v_{M-1}^i) \\
&= (v_M - v_{M-1}) \left(1 - g'(0) - \sum_{i=2}^{d} a_i (v_M^i - v_{M-1}^i) \right). \qquad (2)
\end{aligned}$$

By the induction hypothesis, $v_M - v_{M-1}$ is an element of I^{M-1+n}. Furthermore, $g'(0) \equiv 1 \bmod I$, so $1 - g'(0) \in I$. Finally, since v_M and v_{M-1} are both elements of I^n by (1) and therefore element of I we have $\sum_{i=2}^d a_i(v_M^i - v_{M-1}^i) \in I$. So (2) is an element of I^{M+n}, and by induction we have $v_{m+1} - v_m \in I^{m+n}$ for all $m \in \mathbb{N}$. □

By the previous lemma, $v = (\overline{v}_0, \overline{v}_1, \overline{v}_2, \ldots)$ is an element of the projective limit of R with respect to I, so we can consider it as an element of R since R is complete with respect to I. We will show that $g(v) = (g(\overline{v}_0), g(\overline{v}_1), g(\overline{v}_2), \ldots) = 0$, by proving that $g(v_i) \in I^{n+i}$ for all $i \in \mathbb{N}$. For $i = 0$, we have $g(v_0) = g(0) \in I^n$. Now assume that $g(v_i) \in I^{n+i}$ for all $i < m$. Then we have

$$\begin{aligned}
g(v_m) &= g(v_{m-1} - g(v_{m-1})) \\
&= \sum_{i=0}^{d} a_i (v_{m-1} - g(v_{m-1}))^i \\
&= \sum_{i=0}^{d} a_i (v_{m-1})^i + g(v_{m-1}) \sum_{i=1}^{d} i a_i (v_{m-1})^{i-1} + g(v_{m-1})^2 G(v_{m-1}, g(v_{m-1})) \\
&\quad \text{for a certain } G \in R[x,y] \\
&= g(v_{m-1}) + g(v_{m-1}) g'(v_{m-1}) + g(v_{m-1})^2 G(v_{m-1}, g(v_{m-1})) \\
&= g(v_{m-1})(1 - g'(v_{m-1})) + g(v_{m-1})^2 G(v_{m-1}, g(v_{m-1})). \qquad (3)
\end{aligned}$$

We have $g(v_{m-1}) \in I^{n+m-1}$ by induction. Furthermore, we have $(1 - g'(v_{m-1})) \in I$ since $g'(0) \equiv 1 \bmod I$ and $v_{m-1} \in I$, so $g(v_{m-1})(1 - g'(v_{m-1})) \in I^{n+m}$. Finally, since $g(v_{m-1}) \in I^{n+m-1}$ we have $g(v_{m-1})^2 \in I^{2(n+m-1)} \in I^{n+m}$. So (3) is an element of I^{n+m}. We conclude that $g(v_i) \in I^{n+i}$ for all $i \in \mathbb{N}$, hence $g(v_i) \in I^{1+i}$ for all $i \in \mathbb{N}$, from which it follows that $g(v) = 0$. Since $v_i \in I^n$ for all i, we have $v \in I^n$, so $v \equiv 0 \bmod I^n$. □

As we proved in Example 1.2.7, $\mathbb{Z}_p$ is complete with respect to its ideal $p\mathbb{Z}_p$, so if we have a polynomial in $\mathbb{Z}_p[x]$ and an element $a \in \mathbb{Z}_p$ for which the hypothesis of Hensel's Lemma holds, we can use Hensel's lemma to find a root of this polynomial. It is now clear that Theorem 1.1.18 is in fact Hensel's lemma for the case $n = 1$.

We conclude this section by an application of Hensel's lemma.

Example 1.2.11. Let p be a prime. Using Hensel's lemma, we can determine which elements in $\mathbb{Z}_p$ are squares, i.e. find all elements $0 \neq a \in \mathbb{Z}_p$ for which there exists an $x \in \mathbb{Z}_p$ such that $x^2 - a = 0$. We consider two cases.
First assume that $p \neq 2$. Let $a \in \mathbb{Z}_p$ and assume that a is a square, say $a = b^2$ for a certain $b \in \mathbb{Z}_p$. Write $a = p^n u$, $b = p^m v$ with $n, m \in \mathbb{N}$ and $u, v \in \mathbb{Z}_p^*$. From $a = b^2$ we find $p^n u = p^{2m} v^2$. Since v is a p-adic unit, we see that n is even and u is a square. Consider the polynomial $f(x) = x^2 - u \in \mathbb{Z}_p[x]$ with derivative $f'(x) = 2x$. If u is a square, say $u = w^2$, we have $f(w) = w^2 - u \equiv 0 \bmod p$, hence u is a square modulo p too. So two necessary conditions for a to be is a square is that n is even and u is a square modulo p. To see if these conditions are sufficient, assume that n is even and u is a square modulo p, say $u \equiv w^2 \bmod p$. Then $f(w) = w^2 - u \equiv 0 \bmod p$ and $f'(w) = 2w \neq 0 \bmod p$, so by Hensel's lemma, we know that f has a root in $\mathbb{Z}_p$, hence u is a square in $\mathbb{Z}_p$. This means that $a = p^n u$ is a square in $\mathbb{Z}_p$, too. We conclude that the squares in $\mathbb{Z}_p$ are exactly the elements of the form $a = p^n u$, where u is a p-adic unit that is a square modulo p and n is even.
Now assume that $p = 2$. Let $a \in \mathbb{Z}_2$ and assume that there is a $b \in \mathbb{Z}_2$ such that $a = b^2$. Write $a = p^n u$, $b = p^m v$ for $n, m \in \mathbb{Z}$ and $u, v \in \mathbb{Z}_p^*$. Since v is a p-adic unit, we find $|v|_2 = 1$. So $2 \nmid v$, which means that $v = 2l + 1$ for a certain $l \in \mathbb{Z}_2$. We find $b^2 = p^{2m} v^2 = p^{2m}(2l + 1)^2 = p^{2m}(4l^2 + 4l + 1)$. Since $a = b^2$, it follows that n is even and $u \equiv 1 \bmod 8$. So two necessary conditions for a to be a square in $\mathbb{Z}_2$ are that $u \equiv 1 \bmod 8$ and n is even. To see if these are sufficient, assume that n is even and $u = 8k + 1$ for a certain $k \in \mathbb{Z}_2$. We will show that u is a square in $\mathbb{Z}_2$. Consider the polynomial $f(x) = x^2 - u$. For $m \in \mathbb{Z}_2$, we have $f(2m + 1) = 4m^2 + 4m + 1 - 8k - 1 = 4m^2 + 4m - 8k$. It follows that u is a square in $\mathbb{Z}_2$ if there is an $m \in \mathbb{Z}_2$ such that $g(m) = m^2 + m - 2k = 0$. Since $m^2 + m \equiv 0 \bmod 2$ for all $m \in \mathbb{Z}_2$, we have $g(m) \equiv 0 \bmod 2$ for all $m \in \mathbb{Z}_2$. Moreover, we have $g'(m) = 2m + 1 \not\equiv 0 \bmod 2$ for all $m \in \mathbb{Z}_2$, so Hensel's lemma states that there is an $m \in \mathbb{Z}_2$ for which $g(m) = 0$. It follows that u is a square in $\mathbb{Z}_2$, so $a = p^n u$ is a square in $\mathbb{Z}_p$ too. We conclude that the squares in $\mathbb{Z}_2$ are exactly the elements of the form $a = p^n u$, where n is even and $u \equiv 1 \bmod 8$.

2 Elliptic curves

In this chapter, we will introduce elliptic curves. We will define them, and explain how we can turn an elliptic curve into an abelian group.

2.1 Curves in the projective plane

Let k be an algebraically closed field. We recall that the *affine plane* over k is defined by $\mathbb{A}^2 = \{(x, y)|x, y \in k\}$.

Definition 2.1.1. *Let k be an algebraically closed field. The projective plane over k, denoted by $\mathbb{P}^2(k)$, is defined by*

$$\mathbb{P}^2(k) = \{(a, b, c)|a, b, c \in k, (a, b, c) \neq (0, 0, 0)\}/\sim,$$

where $(a, b, c) \sim (a', b', c') \Leftrightarrow \exists t \in k^* : ta = a', tb = b', tc = c'$.

The equivalence class of a point (a, b, c) in $\mathbb{P}^2(k)$ is denoted by $[a : b : c]$. If k is clear from the context or irrelevant, we often use the notation $\mathbb{P}^2$.

Remark 2.1.2. For a field $k_0 \neq \overline{k}_0$ we denote by $\mathbb{P}^2(k_0)$ the set

$$\mathbb{P}^2(k_0) = \{[a : b : c] \in \mathbb{P}^2(\overline{k}_0)|a, b, c \in k_0\}.$$

Definition 2.1.3. *Let k be an algebraically closed field. A projective line is the set of solutions $[a : b : c] \in \mathbb{P}^2$ of an equation of the form $\alpha X + \beta Y + \gamma Z = 0$, where $[\alpha : \beta : \gamma] \in \mathbb{P}(k)$.*

Remark 2.1.4. The definition of a projective line does not depend on the choice of the representative of points $[a : b : c]$.

Two lines in $\mathbb{P}^2$ intersect each other in exactly one point. Furthermore, there is exactly one line going through any two distinct points in $\mathbb{P}^2$. A projective line is, as we will see, an example of a projective curve.

Definition 2.1.5. *Let k be an algebraically closed field. A polynomial $F \in k[X, Y, Z]$ is called homogeneous of degree d if F is a linear combination of monomials $X^iY^jZ^l$ with $i + j + l = d$.*

Note that the condition in the previous definition implies that for all t we have $F(tX, tY, tZ) = t^dF(X, Y, Z)$. We can now define a *projective curve*.

Definition 2.1.6. *Let k be an algebraically closed field. A projective curve of degree d over k is a set*

$$C = \mathcal{Z}(F) = \{[a : b : c] \in \mathbb{P}^2|F(a, b, c) = 0\},$$

with $F \in k[X, Y, Z]$ a homogeneous polynomial of degree d without repeated factors. If all coefficients of F are in a subring $k' \subset k$, we say that C is defined over k' or that C is a curve over k'.

Remark 2.1.7. The definition of a projective curve does not depend on the choice of the representative of the points $[a : b : c]$.

Remark 2.1.8. Let $C = \mathscr{Z}(f)$ be a curve over a field k. From Hilbert's Nullstellensatz ([2], p.134) it follows that F is uniquely determined by C up to scalar multiplication.

Example 2.1.9. A line in $\mathbb{P}^2$ is a projective curve of degree one.

A projective curve can be intersected with an affine plane to obtain an affine curve. This process is called *dehomogenization*. Let $F(X, Y, Z)$ be a homogeneous polynomial defining a projective curve C. Let $f(x, y) = F(x, y, 1)$ and define the map

$$\phi : \{[a : b : c] \in C | c \neq 0\} \longrightarrow \{(x, y) \in \mathbb{A}^2 | f(x, y) = 0\},$$
$$[a : b : c] \longmapsto \left(\frac{a}{c}, \frac{b}{c}\right).$$

We will prove that ϕ is a bijection. To this end, let $[a : b : c], [a' : b' : c'] \in C$ with $c \neq 0 \neq c'$ and assume that $\phi([a : b : c]) = \phi([a' : b' : c'])$. Then $\frac{a}{c} = \frac{a'}{c'}$ and $\frac{b}{c} = \frac{b'}{c'}$, so $(a, b, c) = \frac{c}{c'}(a', b', c')$, hence $[a : b : c] = [a' : b' : c']$. We conclude that ϕ is injective. For $(x, y) \in \mathbb{A}^2$ with $f(x, y) = 0$ we have $F(x, y, 1) = 0$, hence $\phi([x : y : 1]) = (x, y)$. This means that ϕ is surjective too, so ϕ is bijection between the points $[a : b : c]$ on a projective curve with $c \neq 0$ and a curve in the affine plane. The polynomial f is called the *dehomogenization* of F and the points on C with $c \neq 0$ is called the *affine part* of C. The points on C with $c = 0$ are called *points at infinity* and the projective line given by $Z = 0$ is called the *line at infinity*, denoted by L_∞. We conclude that a projective curve C can be written as a disjoint union of its affine part and its points at infinity.

Conversely, if we start with a curve in the affine plane we can view it as a subset of the projective plane by *homogenization*. Let C be an affine curve defined by the polynomial $f(x, y) = 0$. Write $f(x, y) = \sum a_{ij} x^i y^j$. The *degree* d of $f(x, y)$ as the largest value of $i + j$ for which a_{ij} is not zero. The *homogenization* of $f(x, y)$ is defined by $F(X, Y, Z) = \sum_{i,j} a_{ij} X^i Y^j Z^{d-i-j}$. We see that F is homogeneous of degree d, so $C = \mathscr{Z}(F)$ is a projective curve of degree d.

Remark 2.1.10. We can dehomogenize a projective curve defined by a homogeneous polynomial $F(X, Y, Z)$ by setting $Z = 1$, in which case the line at infinity is given by $L_\infty : Z = 0$. It is important to note here that we could just as well have chosen X or Y instead of Z. However, in this thesis, if we use dehomogenizing we always mean setting $Z = 1$.

Example 2.1.11. Let $F = Y^2Z + aXYZ + bYZ^2 - X^3 - cX^2Z - dXZ^2 - eZ^3$ define a projective curve C over a field k and $P = [0 : 1 : 0] \in C$. The dehomogenization of C with respect to Z is the affine curve $y^2 + axy + by - x^3 - cx^2 - dx - e = 0$. The point P is now a point at infinity. However, if we would have defined dehomogenization with respect to Y, the affine part of C is the curve $z + axz + bz^2 - x^3 - cx^2z - dxz^2 - ez^3 = 0$ and P is the affine point $(x, z) = (0, 0)$.

From the names homogenization and dehomogenization, we would expect these two processes to be inverse to each other. As the next example shows, this is not the case for all curves.

Example 2.1.12. Consider the curve C from example 2.1.11. As we have seen, the dehomogenization of C is given by $y^2 + axy + by - x^3 - cx^2 - dx - e = 0$. If we now homogenize this affine curve, we obtain C again.
Next, consider the curve $C = \mathcal{Z}(F)$ where $F = Z^2Y + ZX^2$. If we dehomogenize C we obtain the affine curve given by $y + x^2 = 0$. But homogenizing this affine curve, we obtain the projective curve given by $ZY + X^2 = 0$, which is not the curve we started with.

From the previous example we see that dehomogenization and homogenization are inverse to each other for all projective curves $C = \mathcal{Z}(F)$ with $Z \nmid F$. However, if we start with an affine curve, the dehomogenization of its homogenization is always the same affine curve.

2.2 Elliptic curves

Definition 2.2.1. *Let C be a projective curve over an algebraically closed field k, defined by a homogeneous polynomial $F(X,Y,Z)$. A point $P \in C$ is called singular if $\frac{\partial F}{\partial X}(P) = \frac{\partial F}{\partial Y}(P) = \frac{\partial F}{\partial Z}(P) = 0$. The curve C is called singular if it contains a singular point and non-singular otherwise.*

Remark 2.2.2. Since F is uniquely determined by C by Remark 2.1.8, the notion of singularity is well-defined.

We can now define one of the main subjects of this thesis: an *elliptic curve*.

Definition 2.2.3. *Let k be an algebraically closed field. An elliptic curve over k is a non-singular projective $E = \mathcal{Z}(F)$ where F is of the form*

$$F = Y^2Z + a_1XYZ + a_3YZ^2 - X^3 - a_2X^2Z - a_4XZ^2 - a_6Z^3 \tag{4}$$

with $a_1, \dots, a_6 \in k$.

We often denote an elliptic curve by its dehomogenization, i.e. we write $E = \mathcal{Z}(f)$ with

$$f = y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6 = 0. \tag{5}$$

Of course, this equation gives only the affine part of an elliptic curve, but to increase readability and since it hardly ever leads to confusion, we will use this equation also to denote the projective curve.

Example 2.2.4. Let $E = \mathcal{Z}(F)$ be an elliptic curve of form (4). We will compute its points at infinity. If we make the substitution $Z = 0$ in (4) we find $X^3 = 0$. This has solution $X = 0$, so an elliptic curve has exactly one point at infinity, the point $[0 : 1 : 0]$. We usually denote this point by $\mathcal{O}$. Note that

$$\frac{\partial F}{\partial Z} = Y^2 + a_1XY + 2a_3YZ - 2a_2X^2 - 2a_4XZ - 3a_6Z^2,$$

hence $\frac{\partial F}{\partial Z}(\mathcal{O}) = 1$, which means that $\mathcal{O}$ is not a singular point.

2.3 The group law of an elliptic curve

Definition 2.3.1. *Let $E = \mathcal{Z}(F)$ be an elliptic curve defined over a field k_0. We define the set $E(k_0)$ as follows.*

$$E(k_0) = \{[a : b : c] \in \mathbb{P}^2(k_0) | F(a, b, c) = 0\}.$$

We call $E(k_0)$ the set of k_0-rational points of E. If $k_0 = \mathbb{Q}$ we call it the set of rational points on E.

Remark 2.3.2. The set $E(k)$ is well-defined by Remark 2.1.8.

Remark 2.3.3. As we will see, if E is an elliptic curve defined over a field k, the set $E(k)$ can be made into an abelian group. To construct the group operation, we need Bézout's theorem, which relates the number of intersections of two projective curves to their degrees. However, the theory that is needed to state Bézout's theorem stretches beyond the contents of this thesis. Therefore, we will state a specific case of Bézout's theorem, that only applies to a line and a projective curve of degree three.

Let L be a line and C a curve in the projective plane over an algebraically closed field k and let $P \in L \cap C$. After making a linear change of coordinates if necessary we can assume that L is the line $Y = 0$ and P is the point $[0 : 0 : 1]$. If we dehomogenize C we obtain its affine part defined by a polynomial $f(x, y) = 0$. If we substitute $y = 0$ into f, we obtain a polynomial $f(x, 0)$ in x.

Definition 2.3.4. *Let L, C, P, f be as above such that the line L is not a component of the curve C. Write $f(x, 0) = x^n g(x, 0)$, where $g(x, 0) \in k[x]$ with $x \nmid g(x, 0)$. The intersection multiplicity $I(L, C, P)$ of L and C at P is defined by $I(L, C, P) = n$. This is independent of the change of variables used.*

Remark 2.3.5. Let C be a curve in the projective plane over an algebraically closed field k. If L is a line that is tangent to C at a point P and that is not a component of C, we have $I(L, C, P) \geq 2$. Furthermore, if M is a line through a singular point S on C that is not a component of C, then $I(M, C, S) \geq 2$.

Theorem 2.3.6 (Special case of Bézout). *Let L be a line and C a curve of degree three in the projective plane over an algebraically closed field k, such that L is not a component of C. Then*

$$\sum_{P \in L \cap C} I(L, C, P) = 3.$$

Proof. See [4], p.20. □

Now we can define our group operation, which we will denote by $+$:

Definition 2.3.7. *Let E be an elliptic curve, and let P and Q be two points on E. If $P \neq Q$, let L be the line through P and Q. If $P = Q$, let L be the tangent line to E at P. According to Bézout's Theorem, there is a unique third point of intersection of E and L, say R. Now let L' be the line through R and $\mathcal{O}$. Again, according to Bézout's theorem, L' intersects E in a unique third point. This point we denote by $P + Q$.*

Theorem 2.3.8. *Let E be an elliptic curve defined over a field k_0. Then $E(k_0)$ is an abelian group under the operation $+$ with identity element $\mathcal{O}$.*

Proof. See [5], p.52. □

We will use the following lemma later on.

Lemma 2.3.9. *Let E be an elliptic curve, L a line, and let $P, Q, R \in E \cap L$. Then $P + Q + R = \mathcal{O}$.*

Proof. First note that R, $\mathcal{O}$ and $P + Q$ are the three points of intersection of E with a line. To add $P + Q$ to R, we construct the line through $P + Q$ and R and take the third point of intersection of this line with E, which is $\mathcal{O}$. If we now construct the line through $\mathcal{O}$ and $\mathcal{O}$ we have the tangent line at $\mathcal{O}$, which is the line at infinity. Since E intersects the line at infinity with multiplicity 3, the third point of intersection of this line and E is again $\mathcal{O}$. So $(P + Q) + R = \mathcal{O}$. □

Example 2.3.10. Let $E = \mathcal{Z}(f)$ be an elliptic curve of form (5) defined over a field k_0 and $P = (\alpha, \beta) \in E(k_0)$. We can derive an explicit formula for $-P$. Let L be the line through P and $\mathcal{O}$ and note that $-P$ is the third point of intersection (say R) of L with E, since $P + R = P + \mathcal{O} + R = \mathcal{O}$. The line L is given by the equation $X = \alpha Z$. So, computing $-P$ means finding the third point of intersection of L and E. If we dehomogenize L we obtain the affine line $x = \alpha$. Substituting this into (5), we find $y^2 + a_1\alpha y + a_3 y - \alpha^3 - a_2\alpha^2 - a_4\alpha - a_6 = 0$. This is a quadratic equation in y where β is a root. Let β' be the other root, then we can write

$$y^2 + a_1\alpha y + a_3 y - \alpha^3 - a_2\alpha^2 - a_4\alpha - a_6 = (y - \beta)(y - \beta') = y^2 - (\beta + \beta')y + \beta\beta'.$$

By comparing the y term we find $-\beta - \beta' = a_1\alpha + a_3$, hence $\beta' = -\beta - a_1\alpha - a_3$. We conclude that $-P$ is given by $-P = (\alpha, -\beta - a_1\alpha - a_3)$.

3 Elliptic curves over $\mathbb{Q}_p$

Let $E = \mathcal{Z}(F)$ be an elliptic curve over $\mathbb{Q}_p$. In this chapter we study the *group of p-adic points* on E given by

$$E(\mathbb{Q}_p) = \{[a : b : c] \in \mathbb{P}^2(\mathbb{Q}_p) | F(a, b, c) = 0\}.$$

This set is an abelian group by Theorem 2.3.8 and in this chapter we describe its structure. First we explain how we can reduce an elliptic curve over $\mathbb{Q}_p$ modulo p. We can then deduce an exact sequence that tells us a lot about $E(\mathbb{Q}_p)$.

3.1 Reduction modulo p

In this section we will define the *reduction modulo p* of an elliptic curve. For an element $x \in \mathbb{Z}_p$ there is a natural reduction map

$$\varphi : \mathbb{Z}_p \longrightarrow \mathbb{F}_p,\ x \longmapsto x \bmod p,$$

where we use the notation $\varphi(x) = \tilde{x}$. There does not exist such a reduction map on $\mathbb{Q}_p$, since all ring homomorphisms on a field are injective. Therefore, it makes sense to consider elliptic curves that are defined over $\mathbb{Z}_p$.

Definition 3.1.1. *Let $E = \mathcal{Z}(f)$ be an elliptic curve of form* (5), *defined over $\mathbb{Z}_p$. The reduction of E, denoted by $\widetilde{E}$, is defined as*

$$\widetilde{E} : \widetilde{f}(x, y) = y^2 + \tilde{a}_1 xy + \tilde{a}_3 y - x^3 - \tilde{a}_2 x^2 - \tilde{a}_4 x - \tilde{a}_6 = 0.$$

We can also reduce the points in $\mathbb{P}^2(\mathbb{Q}_p)$.

Definition 3.1.2. *For $P \in \mathbb{P}^2(\mathbb{Q}_p)$, write $P = [\alpha : \beta : \gamma]$ with $\alpha, \beta, \gamma \in \mathbb{Z}_p$ and at least one of α, β and γ in $\mathbb{Z}_p^*$. The reduction of P, denoted by $\widetilde{P}$, is defined as $\widetilde{P} = [\tilde{\alpha} : \tilde{\beta} : \tilde{\gamma}]$.*

If E is an elliptic curve defined over $\mathbb{Z}_p$ and $P \in E(\mathbb{Q}_p)$, then we have $\widetilde{P} \in \widetilde{E}(\mathbb{F}_p)$. We can now define the *reduction map*

$$\mathbb{P}^2(\mathbb{Q}_p) \longrightarrow \mathbb{P}^2(\mathbb{F}_p)\ , P \longmapsto \widetilde{P}$$

which, when restricted to $E(\mathbb{Q}_p)$, induces a reduction map

$$E(\mathbb{Q}_p) \longrightarrow \widetilde{E}(\mathbb{F}_p)\ , P \longmapsto \widetilde{P}$$

from the p-adic points on an elliptic curve E defined over $\mathbb{Z}_p$ to the points in $\widetilde{E}(\mathbb{F}_p)$.

The following lemma helps us to determine $\widetilde{P}$ for different P.

Lemma 3.1.3. *Let $E = \mathcal{Z}(f)$ be an elliptic curve of form* (5) *defined over $\mathbb{Z}_p$ and $P = (\alpha, \beta)$ a p-adic point on E. Then*

$$\nu_p(\alpha) < 0 \Longrightarrow 2\nu_p(\beta) = 3\nu_p(\alpha).$$

Proof. Write $\alpha = \frac{u}{p^n}, \beta = \frac{v}{p^m}$ with $n \in \mathbb{Z}_{>0}, m \in \mathbb{Z}$ and $u, v \in \mathbb{Z}_P^*$. Since $P \in E$, we have $\nu_p(\beta^2 + a_3\beta + a_1\alpha\beta) = \nu_p(\alpha^3 + a_2\alpha^2 + a_4\alpha + a_6)$. We have

$$\begin{aligned}\nu_p(\beta^2 + a_3\beta + a_1\alpha\beta) &\geq \min\left\{\nu_p\left(\frac{v^2 + a_3vp}{p^{2m}}\right), \nu_p\left(\frac{a_1uv}{p^{n+m}}\right)\right\} \\ &= \min\{-2m, \nu_p(a_1) - n - m\},\end{aligned}$$

since v^2 is not divisible by p, with equality if $\nu_p(\beta^2 + a_3\beta) \neq \nu_p(a_1\alpha\beta)$. On the other hand, we find

$$\nu_p(\alpha^3 + a_2\alpha^2 + a_4\alpha + a_6) = \nu_p\left(\frac{u^3 + a_2u^2p^n + a^4up^{2n} + a_6p^{3n}}{p^{3n}}\right) = -3n,$$

since $n > 0$ and u^3 is not divisible by p. So we have $-3n \geq \min\{-2m, \nu_p(a_1) - n - m\}$. Now assume that $\nu_p(a_1) - n - m \leq -2m$, then have $n \geq m$ (since $a_1 \in \mathbb{Z}_p$) and $-3n \geq \nu_p(a_1) - n - m$. But then $\nu_p(a_1) - m - n \geq -m - n \geq -2n > -3n$ since $n > 0$, which gives a contradiction. We conclude that $\nu_p(a_1) - n - m > -2m$, hence

$$-2m = \nu_p(\beta^2 + a_3\beta + a_1\alpha\beta) = \nu_p(\alpha^3 + a_2\alpha^2 + a_4\alpha + a_6) = -3n,$$

so $2m = 3n$. □

Proposition 3.1.4. *Let E be an elliptic curve defined over $\mathbb{Z}_p$ and $P = (\alpha, \beta) \in E$ with $\alpha, \beta \in \mathbb{Q}_p$. Then $\widetilde{P} = \widetilde{\mathcal{O}}$ if and only if α and β are not both in $\mathbb{Z}_p$.*

Proof. If $\alpha, \beta \in \mathbb{Z}_p$, then $\widetilde{P} = (\tilde{\alpha}, \tilde{\beta})$ with $\tilde{\alpha}, \tilde{\beta} \in \mathbb{F}_p$, so $\widetilde{P} \neq \widetilde{\mathcal{O}}$. If α and β are not both elements of $\mathbb{Z}_p$, by Lemma 3.1.3 we have $\nu_p(\beta) < \nu_p(\alpha)$, from which it follows that $|\beta|_p\alpha \in \mathbb{Z}_p$ and $|\beta|_p\beta \in \mathbb{Z}_p^*$. Write $P = [\alpha : \beta : 1] = [|\beta|_p\alpha : |\beta|_p\beta : |\beta|_p]$. Since p divides $|\beta|_p$ and $|\beta|_p\beta$ is a p-adic unit, we find $\widetilde{P} = [0 : 1 : 0] = \widetilde{\mathcal{O}} \in \widetilde{E}$. So $\widetilde{P} = \widetilde{\mathcal{O}}$ if and only if α and β are not both in $\mathbb{Z}_p$. □

Remark 3.1.5. As we discussed, we can not reduce an elliptic curve E over $\mathbb{Q}_p$ that is not defined over $\mathbb{Z}_p$. However, we can show that such a curve is isomorphic to a curve E' that is defined over $\mathbb{Z}_p$. We can then determine the structure of $E(\mathbb{Q}_p)$ by looking at $E'(\mathbb{Q}_p)$. Let $E = \mathcal{Z}(f)$ be an elliptic curve of form (5), defined over $\mathbb{Q}_p$. By making the change of variables $(x, y) \longmapsto (v^{-2}x, v^{-3}y)$ for a certain $0 \neq v \in \mathbb{Q}_p$, we obtain the elliptic curve

$$E' : f(x, y) = y^2 + a_1vxy + a_3v^3y - x^3 - a_2v^2x^2 - a_4v^4x - a_6v^6 = 0.$$

We can choose v such that $a_iv^i \in \mathbb{Z}_p$ for all i, and thus obtain an equation for E' with all coefficients in $\mathbb{Z}_p$. Since the change of variables is linear and the group law on E and E' is defined in terms of intersections of lines with E and E' respectively, the structure of the group $E(\mathbb{Q}_p)$ is the same as the structure of $E'(\mathbb{Q}_p)$.

3.2 An exact sequence

Let E be an elliptic curve over $\mathbb{Z}_p$ with reduction $\widetilde{E}$. Of course, $\widetilde{E}$ is not always an elliptic curve, since it can contain singular points. We define the following sets:

$$\widetilde{E}_{\mathrm{ns}}(\mathbb{F}_p) = \{P \in \widetilde{E}(\mathbb{F}_p) | P \text{ is not a singular point}\};$$

$$E_0(\mathbb{Q}_p) = \{P \in E(\mathbb{Q}_p) | \widetilde{P} \in \widetilde{E}_{\mathrm{ns}}\};$$
$$E_1(\mathbb{Q}_p) = \{P \in E(\mathbb{Q}_p) | \widetilde{P} = \mathcal{O}\}.$$

Note that by Proposition 3.1.4, we have

$$E_1(\mathbb{Q}_p) = \{P = (\alpha, \beta) \in E(\mathbb{Q}_p) | \alpha \text{ and } \beta \text{ are not both in } \mathbb{Z}_p\}.$$

We will prove that $\widetilde{E}_{\mathrm{ns}}(\mathbb{F}_p)$ can be made into a group by giving it a group structure similar to the group structure of an elliptic curve. Furthermore, we will prove that $E_0(\mathbb{Q}_p)$ and $E_1(\mathbb{Q}_p)$ are subgroups of $E(\mathbb{Q}_p)$. We will then show that the sequence

$$0 \longrightarrow E_1(\mathbb{Q}_p) \longrightarrow E_0(\mathbb{Q}_p) \xrightarrow{\psi} \widetilde{E}_{\mathrm{ns}}(\mathbb{F}_p) \longrightarrow 0,$$

where ψ is the reduction map, is exact. We start by proving that $\widetilde{E}_{\mathrm{ns}}(\mathbb{F}_p)$ can be made into a group.

Definition 3.2.1. *Let E be an elliptic curve over $\mathbb{Z}_p$. We define an operation on $\widetilde{E}_{\mathrm{ns}}$, denoted by $+$, as the operation $+$ on an elliptic curve in Definition 2.3.7.*

Proposition 3.2.2. *Let $E = \mathcal{Z}(f)$ be an elliptic curve of form* (5) *defined over $\mathbb{Z}_p$. The set $\widetilde{E}_{\mathrm{ns}}(\mathbb{F}_p)$ is an abelian group under the operation $+$.*

Proof. Note that $\widetilde{\mathcal{O}}$ is not a singular point, so $\widetilde{\mathcal{O}} \in \widetilde{E}_{\mathrm{ns}}(\mathbb{F}_p)$. Now let $\widetilde{f}$ be the reduction of f modulo p and $\widetilde{P} = (\tilde{\alpha}, \tilde{\beta}) \in \widetilde{E}_{\mathrm{ns}}(\mathbb{F}_p)$. As we showed in Example 2.3.10, we have $-\widetilde{P} = (\tilde{\alpha}, -\tilde{\beta} - \tilde{a}_1\tilde{\alpha} - \tilde{a}_3)$. Since $\widetilde{P}$ is not singular, either $\frac{\partial \widetilde{f}}{\partial x}(\widetilde{P}) \neq 0$ or $\frac{\partial \widetilde{f}}{\partial y}(\widetilde{P}) \neq 0$. First assume that $\frac{\partial \widetilde{f}}{\partial y}(\widetilde{P}) \neq 0$. Then $\frac{\partial \widetilde{f}}{\partial y}(\widetilde{P}) = 2\tilde{\beta} + \tilde{a}_1\tilde{\alpha} + \tilde{a}_3 \neq 0$, hence

$$\frac{\partial \widetilde{f}}{\partial y}(-\widetilde{P}) = 2(-\tilde{\beta} - \tilde{a}_1\tilde{\alpha} - \tilde{a}_3) + \tilde{a}_1\tilde{\alpha} + \tilde{a}_3 = -\frac{\partial \widetilde{f}}{\partial y}(\widetilde{P}) \neq 0,$$

so $-\widetilde{P}$ is not a singular point. If $\frac{\partial \widetilde{f}}{\partial y}(\widetilde{P}) = 0$, then $\frac{\partial \widetilde{f}}{\partial x}(\widetilde{P}) = \tilde{a}_1\tilde{\beta} - 3\tilde{\alpha}^2 - 2\tilde{a}_2\tilde{\alpha} - \tilde{a}_4 \neq 0$, hence

$$\begin{aligned}\frac{\partial \widetilde{f}}{\partial x}(-\widetilde{P}) &= \tilde{a}_1(-\tilde{\beta} - \tilde{a}_1\tilde{\alpha} - \tilde{a}_3) - 3\tilde{\alpha}^2 - 2\tilde{a}_2\tilde{\alpha} - \tilde{a}_4 \\ &= \tilde{a}_1\left(\tilde{\beta} - \frac{\partial \widetilde{f}}{\partial y}(\widetilde{P})\right) - 3\tilde{\alpha}^2 - 2\tilde{a}_2\tilde{\alpha} - \tilde{a}_4 \\ &= \frac{\partial \widetilde{f}}{\partial x}(\widetilde{P}) \neq 0,\end{aligned}$$

so $-\widetilde{P}$ is not a singular point. Hence, for every $\widetilde{P} \in \widetilde{E}_{\mathrm{ns}}(\mathbb{F}_p)$ we have $-\widetilde{P} \in \widetilde{E}_{\mathrm{ns}}(\mathbb{F}_p)$. Finally, we show that $\widetilde{E}_{\mathrm{ns}}(\mathbb{F}_p)$ is closed under the operation $+$. Let $\widetilde{P}, \widetilde{Q} \in \widetilde{E}_{\mathrm{ns}}(\mathbb{F}_p)$ and let L be the line through $\widetilde{P}$ and $\widetilde{Q}$. If the third point of intersection of L and $\widetilde{E}$ were a singular point S, then the intersection multiplicity of $\widetilde{E}$ and L at S would be bigger than one, so L and $\widetilde{E}$ would intersect in at least four points, counting multiplicities. But this would contradict Bézout's theorem, hence, the third point of intersection of L and $\widetilde{E}$ is not a singular point. Since this point is exactly the point $-(\widetilde{P} + \widetilde{Q})$ by Lemma 2.3.9, we have $-(\widetilde{P} + \widetilde{Q}) \in \widetilde{E}_{\mathrm{ns}}(\mathbb{F}_p)$ and by what we just proved this means that $\widetilde{P} + \widetilde{Q} \in \widetilde{E}_{\mathrm{ns}}(\mathbb{F}_p)$, too. We conclude that $\widetilde{E}_{\mathrm{ns}}(\mathbb{F}_p)$ is an abelian group under the operation $+$. □

Our next step is to prove that $E_0(\mathbb{Q}_p)$ is a subgroup of $E(\mathbb{Q}_p)$ and that the reduction map is a homomorphism. To this end, we first discuss the reduction modulo p of a line. Let

$$L : aX + bY + cZ = 0$$

be a line over $\mathbb{Q}_p$. We can multiply by an element of $\mathbb{Z}_p$ to obtain $a, b, c \in \mathbb{Z}_p$ and at least one of a, b, c in $\mathbb{Z}_p^*$. The reduction of L is $\widetilde{L} : \tilde{a}X + \tilde{b}Y + \tilde{c}Z = 0$. Note that if $P \in L$, then $\widetilde{P} \in \widetilde{L}$. We can now prove the following lemma that we will need later on.

Lemma 3.2.3. *Let $E = \mathcal{Z}(f)$ be an elliptic curve of form (5) defined over $\mathbb{Z}_p$. Let $P, Q \in E_0(\mathbb{Q}_p)$ with $\widetilde{P} = \widetilde{Q}$ and let L be the line through P and Q. Then $\widetilde{L}$ is tangent to $\widetilde{E}$ at $\widetilde{P}$.*

Proof. First consider the case where $\widetilde{P} \neq \widetilde{\mathcal{O}}$. Let $\widetilde{f}$ be the reduction of f and write $P = (\alpha, \beta), Q = (\alpha + \mu, \beta + \lambda)$. Since $\widetilde{P} \neq \mathcal{O}$ we have $\alpha, \beta \in \mathbb{Z}_p$ and from $\widetilde{P} = \widetilde{Q}$ it follows that $\lambda, \mu \in p\mathbb{Z}_p$. Because $P \in E_0(\mathbb{Q}_p)$, we have $\widetilde{P} \in \widetilde{E}_{\text{ns}}(\mathbb{F}_p)$, so either $\frac{\partial \widetilde{f}}{\partial y}(\widetilde{P}) \neq 0$ or $\frac{\partial \widetilde{f}}{\partial x}(\widetilde{P}) \neq 0$. By symmetry we can assume that $\frac{\partial \widetilde{f}}{\partial y}(\widetilde{P}) \neq 0$. We will find the slope of the tangent line to $\widetilde{E}$ at $\widetilde{P}$. To this end, first we prove that $\frac{\lambda}{\mu} \in \mathbb{Z}_p$. By writing down the Taylor expansion of f about the point P, we find

$$f(x, y) = f(\alpha, \beta) + (x - \alpha)\frac{\partial f}{\partial x}(\alpha, \beta) + (y - \beta)\frac{\partial f}{\partial y}(\alpha, \beta) + A(x, y),$$

where $A(x, y) \in \mathbb{Z}_p[x, y]$ is a polynomial with only monomials of degree two and higher. Hence

$$0 = f(Q) = \mu\frac{\partial f}{\partial x}(\alpha, \beta) + \lambda\frac{\partial f}{\partial y}(\alpha, \beta) + a\mu^2 + b\mu\lambda + c\lambda^2,$$

with $a, b, c \in \mathbb{Z}_p$. From $\frac{\partial \widetilde{f}}{\partial y}(\widetilde{P}) \neq 0$ and $\frac{\partial f}{\partial y}(P) \in \mathbb{Z}_p$ (since $\alpha, \beta \in \mathbb{Z}_p$) it follows that $\nu_p(\frac{\partial f}{\partial y}(P)) = 0$, so we have

$$\begin{aligned}\nu_p(\lambda) = \nu_p\left(\lambda\frac{\partial f}{\partial y}(P)\right) &= \nu_p\left(\mu\frac{\partial f}{\partial x}(P) + a\mu^2 + b\mu\lambda + c\lambda^2\right) \\ &\geq \min\left\{\nu_p\left(\mu\frac{\partial f}{\partial x}(\alpha, \beta)\right), \nu_p(a\mu^2), \nu_p(b\mu\lambda), \nu_p(c\lambda^2)\right\} \\ &\geq \nu_p(\mu),\end{aligned}$$

since $\nu_p(\lambda) < \nu_p(c\lambda^2)$ and $\frac{\partial f}{\partial x}(\alpha, \beta), \lambda, \mu, a, b, c \in \mathbb{Z}_p$. Hence, $\nu_p(\lambda) \geq \nu_p(\mu)$, so $\frac{\lambda}{\mu} \in \mathbb{Z}_p$. This means that we can reduce $\frac{\lambda}{\mu}$ modulo p. We find:

$$\begin{aligned}0 &= \mu\frac{\partial f}{\partial x}(\alpha, \beta) + \lambda\frac{\partial f}{\partial y}(\alpha, \beta) + a\mu^2 + b\mu\lambda + c\lambda^2 \\ &= \frac{\partial f}{\partial x}(\alpha, \beta) + \frac{\lambda}{\mu}\frac{\partial f}{\partial y}(\alpha, \beta) + a\mu + b\lambda + c\lambda\frac{\lambda}{\mu} \\ &\equiv \frac{\partial f}{\partial x}(\alpha, \beta) + \frac{\lambda}{\mu}\frac{\partial f}{\partial y}(\alpha, \beta) \bmod p\mathbb{Z}_p,\end{aligned}$$

since $\lambda, \mu \in p\mathbb{Z}_p$. We can now determine the slope of the tangent line to $\widetilde{E}$ at $\widetilde{P}$ by setting

$$\frac{dy}{dx}(\widetilde{P}) = -\frac{\frac{\partial \widetilde{f}}{\partial x}}{\frac{\partial \widetilde{f}}{\partial y}}(\widetilde{P}) = \widetilde{\lambda/\mu}.$$

What is left to prove is that the reduction of the line L through P and Q is the line through $\widetilde{P}$ with slope $\widetilde{\lambda/\mu}$. Write $L : y = nx + m$, where $n, m \in \mathbb{Z}_p$. We calculate the slope n by $n = \frac{\beta+\lambda-\beta}{\alpha+\mu-\alpha} = \frac{\lambda}{\mu}$. So $\widetilde{L}$ has slope $\widetilde{\lambda/\mu}$, hence $\widetilde{L}$ is tangent to $\widetilde{E}$ at $\widetilde{P}$. This proves the lemma for $\widetilde{P} \neq \widetilde{O}$.
Now assume that $\widetilde{P} = \widetilde{\mathcal{O}}$. We can make a linear change of variables such that P is the point $(0, 0)$ on a curve isomorphic to E. Now the reduction of P is the affine point $\widetilde{P} = (\tilde{0}, \tilde{0})$, hence we can apply the same reasoning as before. □

Proposition 3.2.4. *Let $E = \mathcal{Z}(f)$ be an elliptic curve of form (5) defined over $\mathbb{Z}_p$. The set $E_0(\mathbb{Q}_p)$ is a subgroup of $E(\mathbb{Q}_p)$ and the map*

$$E_0(\mathbb{Q}_p) \longrightarrow \widetilde{E}_{\text{ns}}(\mathbb{F}_p)\ , P \longmapsto \widetilde{P}$$

is a homomorphism.

Proof. First note that we have $\widetilde{\mathcal{O}} \in \widetilde{E}_{\text{ns}}(\mathbb{F}_p)$ by Proposition 3.2.2, which means that $\mathcal{O} \in E_0(\mathbb{Q}_p)$. Moreover, for $P = [\alpha : \beta : \gamma] \in E(\mathbb{Q}_p)$ we have $\widetilde{P} = [\tilde{\alpha} : \tilde{\beta} : \tilde{\gamma}]$, so $-\widetilde{P} = [\tilde{\alpha} : -\tilde{\beta} - \tilde{a_1}\tilde{\alpha} - \tilde{a_3} : \tilde{\gamma}] = \widetilde{-P} \in \widetilde{E}_{\text{ns}}(\mathbb{F}_p)$. This means that $-P \in E_0(\mathbb{Q}_p)$. Now let $P_1, P_2 \in E_0(\mathbb{Q}_p)$. We will prove that $\widetilde{P_1 + P_2} = \widetilde{P_1} + \widetilde{P_2}$ hence $P_1 + P_2 \in E_0(\mathbb{Q}_p)$, or in other words, the reduction map is a homomorphism and $E_0(\mathbb{Q}_p)$ is closed under addition. To this end, let $P_3 \in E(\mathbb{Q}_p)$ such that $P_1 + P_2 + P_3 = \mathcal{O}$. Then there is a line L such that $P_1, P_2, P_3 \in L$, hence $\widetilde{P_1}, \widetilde{P_2}, \widetilde{P_3} \in \widetilde{L}$. We will prove that $\widetilde{P_1} + \widetilde{P_2} + \widetilde{P_3} = \widetilde{O}$ by distinguishing six different cases.
First assume that $\widetilde{P_1}, \widetilde{P_2}$ and $\widetilde{P_3}$ are all distinct. Then, since they are all on $\widetilde{L}$, we have $\widetilde{P_1} + \widetilde{P_2} + \widetilde{P_3} = \mathcal{O}$.
Secondly, assume that P_1, P_2 and P_3 are all distinct and $\widetilde{P_1} = \widetilde{P_2} \neq \widetilde{P_3}$. Then, by Lemma 3.2.3, the line $\widetilde{L}$ is tangent to $\widetilde{E}$ at $\widetilde{P_1}$, so $\widetilde{L}$ and $\widetilde{E}$ intersect at $\widetilde{P_1}$ with multiplicity bigger or equal to two. From the fact that $\widetilde{P_1} \neq \widetilde{P_3} \in L$ and Bézout's theorem it follows that the intersection multiplicity at $\widetilde{P_1}$ can not be bigger than two. Hence, $2\widetilde{P_1} + \widetilde{P_3} = \widetilde{P_1} + \widetilde{P_2} + \widetilde{P_3} = \widetilde{\mathcal{O}}$.
Thirdly, assume that P_1, P_2 and P_3 are all distinct and $\widetilde{P_1} = \widetilde{P_2} = \widetilde{P_3}$. By Lemma 3.2.3, $\widetilde{L}$ is tangent to $\widetilde{E}$ at $\widetilde{P_1}$, hence has intersection multiplicity bigger or equal to two at $\widetilde{P_1}$. Assume that $\widetilde{L}$ intersects $\widetilde{E}$ at another point Q. If Q were a singular point, then the intersection multiplicity of $\widetilde{L}$ and $\widetilde{E}$ at Q would be bigger then one, so $\widetilde{L}$ would intersect $\widetilde{E}$ in more than three points, counting multiplicities. But this contradicts Bézout's theorem, so Q is not a singular point. This means that the intersection multiplicity of $\widetilde{L}$ and $\widetilde{E}$ at Q is one. We make a change of coordinates such that L is mapped to the line $Y = 0$ and Q is mapped to the point $[0 : 0 : 1]$. Let $f(x, y)$ be the polynomial in $\mathbb{Z}[x, y]$ that defines the dehomogenization of E, then $f(x, 0)$ is a polynomial in $\mathbb{Z}[x]$ which roots are the x-coordinates of the points of intersection of L and E. Since $\widetilde{L}$ and $\widetilde{E}$ intersect at $[0 : 0 : 1]$ with intersection multiplicity one, we have $\widetilde{f} = x\widetilde{g}(x)$ in $\mathbb{F}_p[x]$, where $\widetilde{g} \in \mathbb{F}_p[x]$ and $x \nmid \widetilde{g}$. So $f(0) \equiv 0$

mod p and $f'(0) \not\equiv 0$ mod p, hence by Hensel's lemma there is an $a \in \mathbb{Z}_p$ such that $f(a) = 0$ and $a \equiv 0$ mod p. This means that E and L intersect at the point $[a : 0 : 1]$. But this point is unequal to the images of P_1, P_2 and P_3 under the transformation we performed, since the reduction of $[a : 0 : 1]$ is the point $[0 : 0 : 1]$, which is by assumption not the image under the trasformation of the point $\widetilde{P}_1$. So there is a fourth point of intersection of E and L, which contradicts Bézout's Theorem. We conclude that $\widetilde{P}_1$ is the only point of intersection of $\widetilde{E}$ with $\widetilde{L}$. By Bézout's Theorem this means that $3\widetilde{P}_1 = \widetilde{P}_1 + \widetilde{P}_2 + \widetilde{P}_3 = \mathcal{O}$.
Now assume that $P_1 = P_2 \neq P_3$ and $\widetilde{P_1} = \widetilde{P_2} \neq \widetilde{P_3}$. Since $P_1 = P_2$, the line L is the tangent line at P_1. This means that $\widetilde{L}$ is tangent at $\widetilde{P_1}$, and since $\widetilde{P_1} \neq \widetilde{P_3} \in \widetilde{L}$ we have $2\widetilde{P_1} + \widetilde{P_3} = \widetilde{P_1} + \widetilde{P_2} + \widetilde{P_3} = \widetilde{\mathcal{O}}$.
In the fifth case, assume that $P_1 = P_2 \neq P_3$ and $\widetilde{P_1} = \widetilde{P_2} = \widetilde{P_3}$. This is proved in the same way as the third case.
Finally, if $P_1 = P_2 = P_3$ then L intersects E at P_1 with multiplicity three, from which it follows that $\widetilde{L}$ intersects $\widetilde{E}$ at $\widetilde{P_1}$ with multiplicity three, so $3\widetilde{P_1} = \widetilde{P_1} + \widetilde{P_2} + \widetilde{P_3} = \widetilde{\mathcal{O}}$.
We now proved that $\widetilde{P_1} + \widetilde{P_2} + \widetilde{P_3} = \widetilde{\mathcal{O}}$ in all cases. Since $\widetilde{P_1}, \widetilde{P_2} \in \widetilde{E}_{\text{ns}}(\mathbb{F}_p)$, we find $\widetilde{P_3} = -(\widetilde{P_1} + \widetilde{P_2}) \in \widetilde{E}_{\text{ns}}(\mathbb{F}_p)$, so $P_1 + P_2 = -P_3 \in E_0(\mathbb{Q}_p)$. This means that $E_0(\mathbb{Q}_p)$ is a subgroup of $E(\mathbb{Q}_p)$. Furthermore, we have $\widetilde{P_1 + P_2} = \widetilde{-P_3} = -\widetilde{P_3} = \widetilde{P_1} + \widetilde{P_2}$, hence the reduction map is a group homomorphism. □

We have proved that $E_0(\mathbb{Q}_p)$ and $\widetilde{E}_{\text{ns}}(\mathbb{F}_p)$ are groups and the reduction map is a group homomorphism. It follows by definition that $E_1(\mathbb{Q}_p)$ is the kernel of the reduction map, hence a group, too. We will now prove that the reduction map ψ is surjective.

Proposition 3.2.5. *Let $E = \mathcal{Z}(f)$ be an elliptic curve of form* (5) *defined over $\mathbb{Z}_p$. Then the map*

$$E(\mathbb{Q}_p) \longrightarrow \widetilde{E}_{\text{ns}}(\mathbb{F}_p)\ , P \longmapsto \widetilde{P}$$

is surjective.

Proof. We have $\mathcal{O} \longmapsto \widetilde{\mathcal{O}}$. Let $\widetilde{P} = (\tilde{\alpha}, \tilde{\beta}) \in \widetilde{E}_{\text{ns}}(\mathbb{F}_p)$. Since $\widetilde{P}$ is not singular, either $\frac{\partial \tilde{f}}{\partial x}(\widetilde{P}) \neq 0$ or $\frac{\partial \tilde{f}}{\partial y}(\widetilde{P}) \neq 0$. By symmetry we can assume that $\frac{\partial \tilde{f}}{\partial y}(\widetilde{P}) \neq 0$. Let $a \in \mathbb{Z}_p$ with $\tilde{a} = \tilde{\alpha}$ and consider the polynomial $f(a, y) \in \mathbb{Z}_p[y]$. Note that $\tilde{f}(\tilde{a}, \tilde{\beta}) = 0$ since $\widetilde{P} \in \widetilde{E}_{\text{ns}}(\mathbb{F}_p)$, and $\frac{\partial \tilde{f}}{\partial y}(\tilde{a}, \tilde{\beta}) \neq 0$ by assumption, so by Hensel's lemma there exists a $b \in \mathbb{Z}_p$ with $\tilde{b} = \tilde{\beta}$ and $f(a, b) = 0$, hence $(a, b) \in E(\mathbb{Q}_p)$. We find $(\tilde{a}, \tilde{b}) = \widetilde{P}$, so the reduction map $E(\mathbb{Q}_p) \longrightarrow \widetilde{E}_{\text{ns}}(\mathbb{F}_p)\ , P \longmapsto \widetilde{P}$ is surjective. □

By what we proved above, for an elliptic curve over $\mathbb{Z}_p$ we have an exact sequence

$$0 \longrightarrow E_1(\mathbb{Q}_p) \longrightarrow E_0(\mathbb{Q}_p) \xrightarrow{\psi} \widetilde{E}_{\text{ns}}(\mathbb{F}_p) \longrightarrow 0,$$

where ψ is the reduction map. This means that

$$E_0(\mathbb{Q}_p)/E_1(\mathbb{Q}_p) \cong \widetilde{E}_{\text{ns}}(\mathbb{F}_p).$$

About $E_1(\mathbb{Q}_p)$ we know the following:

Proposition 3.2.6. *Let p be an odd prime and let E be an elliptic curve over $\mathbb{Z}_p$. Then $E_1(\mathbb{Q}_p) \cong \mathbb{Z}_p$.*

Proof. See [5], p.191. □

As the following proposition shows, we can now explicitly calculate $E(\mathbb{Q}_p)$ for a large class of elliptic curves.

PROPOSITION 3.2.7. *Let p be an odd prime and let E be an elliptic curve over $\mathbb{Z}_p$ for which $\widetilde{E}$ is an elliptic curve too. Furthermore, assume that there is a homomorphism $s : \widetilde{E}(\mathbb{F}_p) \longrightarrow E(\mathbb{Q}_p)$ such that $\psi \circ s = \mathrm{id}_{\widetilde{E}(\mathbb{F}_p)}$, where ψ is the reduction map. Then we have*

$$E(\mathbb{Q}_p) \cong \mathbb{Z}_p \times \widetilde{E}(\mathbb{F}_p).$$

Proof. Since $\widetilde{E}$ is non-singular, we have $E_0(\mathbb{Q}_p) = E(\mathbb{Q}_p)$ and $\widetilde{E}_{\mathrm{ns}}(\mathbb{F}_p) = \widetilde{E}(\mathbb{F}_p)$, so we have an exact sequence

$$0 \longrightarrow \mathbb{Z}_p \longrightarrow E(\mathbb{Q}_p) \longrightarrow \widetilde{E}(\mathbb{F}_p) \longrightarrow 0.$$

Furthermore, since s is a section this sequence splits. □

We know the group $\mathbb{Z}_p$, and the group $\widetilde{E}(\mathbb{F}_p)$ is easily calculated since it is finite. So in the case of the previous proposition, we know exactly what the structure of $E(\mathbb{Q}_p)$ is. In the next section we give two examples where this is the case.

3.3 Two examples

EXAMPLE 3.3.1. Consider the elliptic curve

$$E : f(x, y) = y^2 - x^3 + 2x = 0$$

over $\mathbb{Q}_3$. If we reduce E modulo 3 (this is possible since E is defined over $\mathbb{Z}_3$) we obtain the reduced curve

$$\widetilde{E} : \tilde{f}(x, y) = y^2 - x^3 + \tilde{2}x = 0.$$

Note that $\frac{\partial \tilde{f}}{\partial x}(x, y) = \tilde{2} \neq \tilde{0}$, so $\widetilde{E}$ is an elliptic curve, too. As we have seen in the previous section, we now have an exact sequence

$$0 \longrightarrow \mathbb{Z}_3 \longrightarrow E(\mathbb{Q}_3) \longrightarrow \widetilde{E}(\mathbb{F}_3) \longrightarrow 0.$$

We will prove that this sequence splits by constructing a section. First, we calculate the group $\widetilde{E}(\mathbb{F}_3)$ and find

$$\widetilde{E}(\mathbb{F}_3) = \{(\tilde{2}, \tilde{1}), (\tilde{0}, \tilde{0}), (\tilde{2}, -\tilde{1}), \mathcal{O}\}.$$

So $\widetilde{E}(\mathbb{F}_3)$ is a group of order four, which means that it is isomorphic to either C_4 or V_4. We can tell which one by finding the points of order two in $\widetilde{E}(\mathbb{F}_3)$. A point $\mathcal{O} \neq P$ is of order two if and only if $P = -P$. As we have showed in Example 2.3.10, for a point $P = (\tilde{\alpha}, \tilde{\beta}) \in \widetilde{E}(\mathbb{F}_3)$ we have $-P = (\tilde{\alpha}, -\tilde{\beta})$, so P is of order two if and only if $\tilde{\beta} = -\tilde{\beta}$, which implies $\tilde{\beta} = \tilde{0}$. This means that $\widetilde{E}(\mathbb{F}_3)$ contains exactly one point of order two, which is the point $(\tilde{0}, \tilde{0})$. Since V_4 has three points of order two, we conclude that $\widetilde{E}(\mathbb{F}_3) \cong C_4$.
Our next step is to construct a section $s : \widetilde{E}(\mathbb{F}_3) \longrightarrow E(\mathbb{Q}_3)$. Since $(\tilde{2}, \tilde{1})$ is a

point of order four, hence a generator of $\widetilde{E}(\mathbb{F}_3)$, the homomorphism s is completely determined by $s(\tilde{2},\tilde{1})$. We find a point of order four in $E(\mathbb{Q}_3)$ by using the fourth *division polynomial* of E, denoted by ψ_4, which is a polynomial whose roots are the x-coordinates of the 4-torsion points of E unequal to $\mathcal{O}$ (see [5], p.373). We calculate $\psi_4(x)$ using Sage (see the appendix) and after dividing out the polynomial $\psi_2 = x^3 - 2x$ (since 2-torsion points have y-coordinate equal to zero) we find that the x-coordinates of points of order four are the roots of the polynomial

$$f(x) = x^6 - 10x^4 - 20x^2 + 8.$$

Note that $f(2) = -168 \equiv 0 \bmod 3$ (which confirms that $(\tilde{2},\tilde{1})$ is a point of order 4 in $E(\mathbb{F}_3)$) and $f'(2) = -200 \not\equiv 0 \bmod 3$, so we can use Hensel's lemma to find a point $a \in \mathbb{Z}_3$ such that $f(a) = 0$ and $\tilde{a} = \tilde{2}$. Therefore, the equation $y^2 = a^3 - 2a$ has a solution modulo 3, hence by Example 1.2.11 it has a solution in $\mathbb{Z}_3$. So there is a b in $\mathbb{Z}_3$ such that $(a,b) \in E(\mathbb{Q}_3)$ is a point of order four with $(\tilde{a},\tilde{b}) = (\tilde{2},\tilde{1}) \in E(\mathbb{F}_3)$. If we let $s(\tilde{2},\tilde{1}) = (a,b)$, then $(\psi \circ s)(\tilde{2},\tilde{1}) = (\tilde{2},\tilde{1})$ (where ψ is the reduction map). Since s and ψ are homomorphisms and $(\tilde{2},\tilde{1})$ generates $E(\mathbb{F}_3)$, we find $(\psi \circ s)(P) = P$ for all $P \in E(\mathbb{F}_3)$. Hence, $\psi \circ s = \mathrm{id}_{\widetilde{E}(\mathbb{F}_3)}$, so by Proposition 3.2.7 we have

$$E(\mathbb{Q}_3) \cong \mathbb{Z}_3 \times C_4.$$

Example 3.3.2. Consider the elliptic curve

$$E : f(x,y) = y^2 - x^3 - x^2 - x - 1 = 0$$

over $\mathbb{Q}_5$. Since E is defined over $\mathbb{Z}_5$, we can reduce E modulo 5 to obtain

$$\widetilde{E} : \tilde{f}(x,y) = y^2 - x^3 - x^2 - x - \tilde{1} = 0.$$

We have $\frac{\partial \tilde{f}}{\partial x} = -\tilde{3}x^2 - \tilde{2}x - \tilde{1}$ and $\frac{\partial \tilde{f}}{\partial y} = \tilde{2}y$, so $\frac{\partial \tilde{f}}{\partial y} = \tilde{2}y = \tilde{0}$ implies $y = \tilde{0}$. The points on $\widetilde{E}$ with y-coordinate equal to zero are $(\tilde{2},\tilde{0})$, $(\tilde{3},\tilde{0})$ and $(\tilde{4},\tilde{0})$, which do all have $\frac{\partial \tilde{f}}{\partial x} \neq \tilde{0}$, so $\widetilde{E}$ does not contain any singular points, hence it is an elliptic curve. This gives us the exact sequence

$$0 \longrightarrow \mathbb{Z}_5 \longrightarrow E(\mathbb{Q}_5) \longrightarrow \widetilde{E}(\mathbb{F}_5) \longrightarrow 0.$$

We find

$$\widetilde{E}(\mathbb{F}_5) = \{(\tilde{0},\tilde{1}), (\tilde{0},\tilde{4}), (\tilde{1},\tilde{2}), (\tilde{1},\tilde{3}), (\tilde{2},\tilde{0}), (\tilde{3},\tilde{0}), (\tilde{4},\tilde{0}), \mathcal{O}\}.$$

Since $\widetilde{E}(\mathbb{F}_5)$ is a group of order eight, it is isomorphic to either C_8, $C_4 \times C_2$ or $C_2 \times C_2 \times C_2$. The points of order two are again the points with y-coordinate equal to zero, so we see that $\widetilde{E}(\mathbb{F}_5)$ contains exactly three points of order two. Since C_8 has one point of order two and $C_2 \times C_2 \times C_2$ contains seven points of order two, we conclude that $\widetilde{E}(\mathbb{F}_5)$ is isomorphic to $C_4 \times C_2$.

We will construct a section $s : \widetilde{E}(\mathbb{F}_5) \longrightarrow E(\mathbb{Q}_5)$. By a simple calculation (see [6], p.31) we find $2(\tilde{0},\tilde{1}) = 2(\tilde{0},\tilde{4}) = 2(\tilde{1},\tilde{2}) = 2(\tilde{1},\tilde{3}) = (\tilde{3},\tilde{0})$, so any point of order two unequal to $(\tilde{3},\tilde{0})$ together with a point of order four generates $\widetilde{E}(\mathbb{F}_5)$. We will take the points $(\tilde{2},\tilde{0})$ and $(\tilde{0},\tilde{1})$. Now s is determined by $s(\tilde{2},\tilde{0})$ and $s(\tilde{0},\tilde{1})$, so we will find a point of order two and a point of order four in $E(\mathbb{Q}_5)$. Note that $\psi_2 = x^3 + x^2 + x + 1$, since points of order two have y-coordinate equal to zero. We have $\psi_2(2) = 15 \equiv 0 \bmod 5$ and $\psi_2'(2) = 17 \not\equiv 0 \bmod 5$, so Hensel's lemma gives us a point $a \in \mathbb{Z}_5$ with $\psi_2(a) = 0$ and $\tilde{a} = \tilde{2}$. This means that $y^2 = a^3 + a^2 + a + 1$ has a solution modulo 5, so by Example 1.2.11 it has a solution b in $\mathbb{Z}_5$, too. It follows that there is a point $(a, b) \in E(\mathbb{Q}_5)$ of order two with $(\tilde{a}, \tilde{b}) = (\tilde{2}, \tilde{0})$. To find a point of order four in $E(\mathbb{Q}_5)$, we calculate ψ_4 (see the appendix). After dividing out ψ_2 we find that the x-coordinates of the points of order four on E are the roots of the polynomial

$$f(x) = x^6 + 2x^5 + 5x^4 + 20x^3 + 15x^2 + 2x - 5.$$

We have $f(0) = -5 \equiv 0 \bmod 5$ and $f'(0) = -3 \not\equiv 0 \bmod 5$, so we can again apply Hensel's lemma to find a point $c \in \mathbb{Z}_5$ with $f(c) = 0$ and $\tilde{c} = \tilde{0}$. Analogous to what we have done above, this means that there is a point $(c, d) \in E(\mathbb{Q}_p)$ of order four with $(\tilde{c}, \tilde{d}) = (\tilde{0}, \tilde{1})$. We let $s(\tilde{2}, \tilde{0}) = (a, b)$ and $s(\tilde{0}, \tilde{1}) = (c, d)$. We have $(\psi \circ s)(\tilde{2}, \tilde{0}) = (\tilde{2}, \tilde{0})$ and $(\psi \circ s)(\tilde{0}, \tilde{1}) = (\tilde{0}, \tilde{1})$ and since ψ and s are homomorphisms and $(\tilde{2}, \tilde{0})$ and $(\tilde{0}, \tilde{1})$ generate $\widetilde{E}(\mathbb{F}_5)$, we have $(\psi \circ s)(P) = P$ for all $P \in \widetilde{E}(\mathbb{F}_5)$. We conclude that $\psi \circ s = \mathrm{id}_{\widetilde{E}(\mathbb{F}_5)}$, so by Proposition 3.2.7 we have

$$E(\mathbb{Q}_5) \cong \mathbb{Z}_5 \times C_4 \times C_2.$$

Literature

[1] J.W.S. Cassels, *Lectures on Elliptic Curves*, Cambridge University Press, Cambridge, first edition, 1991.

[2] D. Eisenbud, *Commutative Algebra with a View Toward Algebraic Geometry*, Springer-Verlag, New York, 1995.

[3] F. Q. Gouvêa, *p-adic Numbers, An Introduction*, Springer-Verlag, Germany, second edition, 1997.

[4] I.R. Shafarevich, *Basic Algebraic Geometry 1*, Springer-Verlag, Germany, second edition, 1994.

[5] J.H. Silverman, *The Arithmetic of Elliptic Curves*, Springer, New York, second edition, 2009.

[6] J. H. Silverman and J. Tate, *Rational Points on Elliptic Curves*, Springer-Verlag, New York, 1992.

Appendix

Sage code used in Example 3.3.1

```
E1=EllipticCurve(QQ,[0,0,0,-2,0]);
f=E1.division_polynomial(4);
f.factor()
```

Sage code used in Example 3.3.2

```
E1=EllipticCurve(QQ,[0,1,0,1,1]);
f=E1.division_polynomial(4);
f.factor()
```