Local fields and the Hasse principle

Alvaro Gonzalez Hernandez

MSc in Mathematical Sciences
Trinity Term 2021

Abstract

In the present dissertation, we will discuss the main results of the theory of local fields and its connections to the study of elliptic curves, in particular, to the computation of their rank by the method of complete 2-descent.

The knowledge gained from this theory will be used to analyse a family of counter-examples to the Hasse principle depending on a prime parameter p. This family of curves arises as the homogeneous spaces that appear when applying complete 2-descent on an elliptic curve $\mathcal{E}$ of the form $y^2 = x(x-p)(x-p-8)$ with non-trivial Tate-Shafarevich group.

The 2-Selmer groups of $\mathcal{E}$ over the fields $K = \mathbb{Q}$ and $K = \mathbb{Q}(i)$ are explicitly computed by finding sets of generators of the groups $\mathcal{E}(K_\mathfrak{p})/2\mathcal{E}(K_\mathfrak{p})$ for every Archimedean place and every prime $\mathfrak{p}$ of bad reduction of $\mathcal{E}$. By studying the quadratic twist of $\mathcal{E}$ with respect to -1 and analysing the rank bounds given by all the 2-Selmer groups, we give a description of the rank and the 2-torsion part of the Tate-Shaferevich group of $\mathcal{E}$ based on the properties of p.

Contents

1 Introduction

The study of Diophantine equations, that is, the solutions of equations in the integers or the rationals, has fascinated many mathematicians in history.

The main difficulty of working with rational numbers, unlike working with real numbers, is their lack of completeness. This entails that we cannot construct solutions to equations by considering the limit of sequences of approximations. To remedy this situation, mathematicians such as Kurt Hensel and Helmut Hasse started analysing the possible completions of the rationals with respect to absolute values. The resulting fields, known as the ***p*-adic numbers**, are completions with respect to absolute values $|\ \ |_p$ that reflect the multiplicity of a prime p in the factorization of a rational.

The study of the p-adic numbers, and more generally **local fields**, have meanwhile led to solutions of many problems in number theory and geometry. The fundamental question of whether local information suffices to solve a problem in a global setting is now known as the **Hasse principle**. Individual counterexamples to this principle are easy to find, but a more systematic study of complex examples requires a deep understanding of the underlying geometrical concepts.

My goal in this dissertation is to present a family of counterexamples to the Hasse principle. The study of this particular example will showcase the difficulties that arise when working with elliptic curves, and how local fields provide a fundamental tool for understanding them.

2 | Local fields

2.1 Global and local fields

2.1.1 Absolute values on a field

Definition 2.1. *An **absolute value** on a field K is a function*

$$|\ |\colon K \longrightarrow \mathbb{R}_{\geq 0}$$

that satisfies the following conditions:

1. $|x| = 0$ *if and only if* $x = 0$.
2. $|xy| = |x|\,|y|$ *for all* $x, y \in K$.
3. $|x + y| \leq |x| + |y|$ *for all* $x, y \in K$.

*We will say that an absolute value is **non-Archimedean** if it satisfies the condition known as the **ultrametric inequality**:*

4. $|x + y| \leq \max\{|x|, |y|\}$ *for all* $x, y \in K$.

*Otherwise, we will say that $|\ |$ is **Archimedean**.*

Example 2.1. In every field K a **trivial absolute value** can be defined as $|x| = 1$ for $x \neq 0$ and $|0| = 0$.

Example 2.2. In $\mathbb{Q}$ and $\mathbb{R}$ we have the **standard absolute value**, defined as

$$|x|_\infty = \max\{x, -x\}.$$

This is an example of an Archimedean absolute value. We will now see that it is also possible to give $\mathbb{Q}$ a non-Archimedean absolute value.

Example 2.3. Let p be a fixed prime. As $\mathbb{Z}$ is a unique factorization domain, we can express every non-zero rational number as $x = p^n \frac{a}{b} \in \mathbb{Q}$, with $a, b, n \in \mathbb{Z}$ and a, b coprime to p. We can then define a function $v_p : \mathbb{Q} \to \mathbb{R}$ as $v_p(x) = n$.

Definition 2.2. *The **p-adic absolute value** of a rational number x is defined to be*

$$|x|_p = \begin{cases} p^{-v_p(x)} & \text{if } x \neq 0 \\ 0 & \text{if } x = 0 \end{cases}$$

Given an absolute value $|\ |$ on a field K, by defining the distance between any two points $x, y \in K$ as $d(x, y) = |x - y|$, we can give K a structure of **metric space** so, in particular, we can give it a **topological structure**.

We recall that a metric space K is called **complete** with respect to $|\ |$ if every Cauchy sequence of elements has a limit in K. Given a field K with an absolute value $|\ |$, we can always construct a complete extension of K, known as the **completion** of K by considering all the equivalence classes of Cauchy sequences in K under the relation:

$$\{x_n\} \equiv \{y_n\} \Leftrightarrow \{x_n - y_n\} \text{ converges to zero.}$$

The completion of K contains K, as every $x \in K$ can be understood as a constant sequence where all the terms are x. Furthermore, by defining an absolute value on the completion of K by $|\{x_n\}| = \lim_{n\to\infty} |x_n|$, this absolute value restricts to $|\ |$ on K. Then, with respect to $|\ |$, the completion of K is complete and the smallest complete field containing K [Gou20, Section 3.2].

Completions give us better tools to find solutions to equations, as approximations result in convergent sequences. That is the reason why for calculus we use $\mathbb{R}$, the completion of $\mathbb{Q}$, with respect to $|\ |_\infty$.

As mentioned in the introduction, this idea motivated the following definition.

Definition 2.3. *The field of **p-adic numbers** $\mathbb{Q}_p$ is the completion of $\mathbb{Q}$ with respect to the absolute value $|\ |_p$.*

In this dissertation, we will see the importance of $\mathbb{Q}_p$ and other completions of fields with respect to non-Archimedean absolute values.

2.1.2 Valuations and their structures

There is a concept related to non-Archimedean absolute values that will help us to study completions.

Definition 2.4. *A **valuation** on a field K is a function*

$$v\colon K \to \mathbb{R} \cup \{\infty\}$$

that satisfies the following conditions:

1. $v(0) = \infty$.
2. $v(xy) = v(x) + v(y)$ *for all* $x, y \in K$.
3. $v(x + y) \geq \min\{v(x), v(y)\}$ *for all* $x, y \in K$.

For any $0 < c < 1$, $|x|_v := c^{v(x)}$ defines a non-Archimedean absolute value on K. Similarly, for every non-Archimedean value $|\ |$, $v(x) = -\log|x|$ is a valuation.

Example 2.4. The function v_p that we defined in section 2.1 is a valuation.

There are some algebraic structures associated to any field K with a valuation.

Definition 2.5. *The **valuation ring** of K with respect to $|\ |$ is the subring*

$$R_K = \{x \in K : v(x) \geq 0\} \subset K.$$

Definition 2.6. *The **valuation ideal** is the ideal*

$$\mathcal{M}_K = \{x \in K : v(x) > 0\} \subset R_K.$$

If the image of v in $\mathbb{R}$ is isomorphic to $\mathbb{Z}$, then we say that v is a **discrete valuation**. For discrete valuations, v maps R_K surjectively onto $\mathbb{Z}_{\geq 0}$, so there must exist an element $\pi \in R_K$, known as a **uniformizer** such that $v(\pi) = 1$.

In that case it can easily be seen that $\mathcal{M}_K = \pi R_K$ and that $\mathcal{M}_K$ is maximal, so the ring $\kappa = R_K/\mathcal{M}_K$ is a field, known as the **residue field** of K.

As v_p is a discrete valuation, we have the following definition:

Definition 2.7. *The ring of **p-adic integers** is the valuation ring of $\mathbb{Q}_p$:*

$$\mathbb{Z}_p = \{x \in \mathbb{Q}_p : v_p(x) \geq 0\} = \{x \in \mathbb{Q}_p : |x|_p \leq 1\}$$

In this case, p is a uniformizer of $\mathbb{Z}_p$, so we have that $\mathcal{M}_{\mathbb{Q}_p} = p\mathbb{Z}_p$ and $\kappa = \mathbb{Z}/p\mathbb{Z}$.

2.1.3 Characterisation of global and local fields

It is now time to define one of the main objects of study in this dissertation:

Definition 2.8. *A **local field** is a field K with a non-trivial absolute value $|\ |$ which is locally compact, i.e. every point has a compact neighbourhood under the topology induced by $|\ |$.*

From Heine-Borel's theorem, we know that closed intervals in $\mathbb{R}$ are compact so $\mathbb{R}$ is a **local field**. The p-adic fields are also local fields by the following result:

Proposition 2.1. *Let K be a field with an absolute value $|\ |$ induced by a discrete valuation. Then K is a local field if and only if K is complete and the residue field κ is finite.*

Proof. [Sut17, Proposition 9.6] □

In contrast to the term of local fields, we have the following term.

Definition 2.9. *A **global field** is a finite extension of either $\mathbb{Q}$ or $\mathbb{F}_q(t)$, the field of rational functions over $\mathbb{F}_q$ where q is a prime power.*

If K is a global field with absolute value $|\ |$, its completion with respect to $|\ |$ is a local field [Sut17, Corollary 9.7]. To analyse the possible local fields of a global field K, we will study the different absolute values of K.

2.2 Places of a number field

As we are interested in analysing absolute values by the topology they induce, we can consider two absolute values to be equivalent if they define the same topology on K.

Definition 2.10. *The **set of places** of a field K, denoted by M_K, is the set of equivalence classes of non-trivial absolute values on K.*

It is easy to see [Gou20, Proposition 3.1.3] that any two equivalent absolute values on K generate the same completion and we can assign to any place $\mathfrak{p} \in M_K$ a completion, denoted by $K_\mathfrak{p}$, which will be a local field.

In the case of the rationals, $M_\mathbb{Q}$ is given by the following theorem:

Theorem 2.1 (Ostrowski). *Every non-trivial absolute value on $\mathbb{Q}$ is either equivalent to the standard absolute value $|\ |_\infty$ or to $|\ |_p$ for some p prime. Therefore, all the possible completions of $\mathbb{Q}$ with respect to an absolute value are either $\mathbb{R}$ or $\mathbb{Q}_p$ for some prime p.*

Proof. [Gou20, Theorem 3.1.4]. □

In a general setting, studying the set of places of a global field involves analysing the ramification of finite extensions of $\mathbb{Q}_p$ [Cas86, Chapters 7-10]. I will not develop this topic in this dissertation, but I would like to present some of the results of this theory for the case where K is a **number field**.

If L/K is a extension of global fields, for every place $\mathfrak{q}$ of L, any associated absolute value $|\ |_\mathfrak{q}$ restricts to an absolute value on K that represents a place $\mathfrak{p}$ of K [Sut17, Definition 13.4]. This is expressed by saying that $\mathfrak{q}$ **lies above** $\mathfrak{p}$. In the case of number fields $K/\mathbb{Q}$, we therefore have the following possibilities.

2.2.1 The Archimedean case

Let $\mathfrak{p} \in M_K$ lie over the Archimedean place of $\mathbb{Q}$, that we will represent by ∞. As we recall, if $[K : \mathbb{Q}] = n$, there are n distinct embeddings

$$\sigma_j \colon K \to \mathbb{C} \qquad\qquad 1 \leq j \leq n.$$

Among those embeddings, there are r real embeddings (those for which $\sigma_j(K) \subseteq \mathbb{R}$) and s pairs of conjugate complex embeddings, so $n = r + 2s$. By defining an Archimedean absolute value as

$$|x|_j = \left| \operatorname{Re}(\sigma_j(x))^2 + \operatorname{Im}(\sigma_j(x))^2 \right|_\infty^{1/2}$$

each of the real embeddings gives a place under which the completion of K is $\mathbb{R}$, and every pair of conjugate complex embeddings gives a place under which the completion of K is $\mathbb{C}$. These $r + s$ different places are all possible Archimedean places in K [Neu99, Theorem 8.1].

2.2.2 The non-Archimedean case

Let $\mathfrak{p} \in M_K$ lie over a prime p. From the unique factorisation of ideals in K,

$$(p) = \mathfrak{p}_1^{e_1}\mathfrak{p}_2^{e_2}\cdots\mathfrak{p}_r^{e_r}$$

for some prime ideals $\mathfrak{p}_i$ of $\mathcal{O}_K$. Then, every place $\mathfrak{p}$ lying over p corresponds to a prime ideal $\mathfrak{p}_i$ that lies over (p) [Neu99, Proposition 8.5]. The absolute value $|\ |_{\mathfrak{p}_i}$ is defined as

$$|x|_{\mathfrak{p}_i} = p^{-v_{\mathfrak{p}_i}(x)/e_i}$$

where $v_{\mathfrak{p}_i}(x)$ is defined as the power of $\mathfrak{p}_i$ in the prime factorisation of (x) as fractional ideals [Neu99, Section 11]. In that case, for $x \in \mathbb{Q}$, $v_{\mathfrak{p}_i}(x) = v_p(x)e_i$ and $|x|_{\mathfrak{p}_i} = |x|_p$.

Example 2.5. Let us analyse the places of $\mathbb{Q}(i)$.

- As $\mathbb{Q}(i)$ has only a pair of conjugate complex embeddings, it has one Archimedean value, defined as the standard absolute value on $\mathbb{C}$, so $\mathbb{Q}(i)_\infty = \mathbb{C}$.
- $\mathbb{Z}[i]$, on the other hand, is a principal ideal domain, so all ideals are principal and the non-Archimedean places correspond to the primes of $\mathbb{Z}[i]$. We will therefore denote by $\mathbb{Z}[i]_\mathfrak{p}$ the valuation ring of $\mathbb{Q}(i)_\mathfrak{p}$.

2.3 Hensel's lemma

The definition of the completion of a field does not help us to understand the elements of a complete field K. Fortunately, in the case of local fields, the finiteness of the residue field gives us an easy way to do so through the following result:

Proposition 2.2. *Let K a local field with an absolute value $|\ |$ induced by a discrete valuation and let $\{r_1, r_2, \ldots, r_\ell\} \subset R_K$ be a fixed set of representatives for the elements of κ, that is, for the cosets of $\mathcal{M}_K$. If π is a uniformizer of R_K, then any element $x \in K$ has a unique representation as a sum of the form*

$$x = \sum_{j=m}^{\infty} a_j \pi^j$$

where $m \in \mathbb{Z}$ and $a_j \in \{r_1, \ldots, r_\ell\}$. Likewise, every sum defined as before converges to an element of K.

Proof. [Gou20, Proposition 6.4.5]. □

In the case of $\mathbb{Q}_p$, every element $x \in \mathbb{Q}_p$ can be understood as an infinite series

$$x = \sum_{j=m}^{\infty} a_j p^j$$

where $a_j \in \{0, \ldots, p-1\}$ and $m = v_p(x)$.

For example, as $|p^{N+1}|_p \to 0$ when $N+1 \to \infty$,

$$\sum_{j=0}^{\infty}(p-1)\,p^j = (p-1)\lim_{N\to\infty}\sum_{j=0}^{N}p^j = (p-1)\lim_{N\to\infty}\frac{p^{N+1}-1}{(p-1)} = -1.$$

If we did not know this *ad hoc* reasoning to compute the p-adic expansion of -1, we could compute every a_j by solving congruences modulo p^j, as we see in this example when $p=5$,

$$\begin{array}{rcrcrcl}
x &\equiv& -1 &\equiv& 5-1 &\equiv& 4 \pmod 5 \\
x &\equiv& -1 &\equiv& 5^2-1 &\equiv& 4+4\cdot 5 \pmod{5^2} \\
x &\equiv& -1 &\equiv& 5^3-1 &\equiv& 4+4\cdot 5+4\cdot 5^2 \pmod{5^3} \\
x &\equiv& -1 &\equiv& 5^4-1 &\equiv& 4+4\cdot 5+4\cdot 5^2+4\cdot 5^3 \pmod{5^4} \\
\vdots && \vdots && \vdots && \vdots \\
x &=& -1 &=& \sum 4\cdot 5^j &=& 4+4\cdot 5+4\cdot 5^2+4\cdot 5^3+\cdots
\end{array}$$

In $\mathbb{R}$, the Newton-Raphson method allows us to produce a sequence converging to a solution of an equation. In $\mathbb{Q}_p$ and, more generally, in any non-Archimedean local field we have an analogous method:

Theorem 2.2 (Hensel's lemma). *Let $K_{\mathfrak{p}}$ be a local field with a discrete non-Archimedean absolute value $|\ |_{\mathfrak{p}}$ and let $R_{K_{\mathfrak{p}}}$ be its valuation ring. Let $f(x)$ a polynomial with coefficients in $R_{K_{\mathfrak{p}}}$ and let $a_0 \in R_{K_{\mathfrak{p}}}$ such that $|f(a_0)| < |f'(a_0)|^2$, where $f'(x)$ is the formal derivative of $f(x)$. Then, there is an $a \in R_{K_{\mathfrak{p}}}$ such that $f(a)=0$. Furthermore,*

$$|a-a_0| \leq \frac{|f(a_0)|}{|f'(a_0)|}.$$

Proof. In the book of Cassels on local fields, a classical proof of this statement can be found [Cas86, Lemma 3.1]. It is also possible to prove this theorem in a constructive way by showing that the root a of $f(x)$ can be found as the limit of a sequence $\{a_n\}$ defined recursively as

$$a_{n+1} = a_n - \frac{f(a_n)}{f'(a_n)}.$$

This approach and the formulas for the convergence of this sequence can be found in Conrad's article [Con]. □

2.3.1 Applications of Hensel's lemma

We will now see an application of Hensel's lemma on how to find the set of squares of a local field.

Proposition 2.3. *An element $b \in \mathbb{Q}_2$ is a square if and only if it is of the form $b = 2^n b_0$ with n an even integer and $b_0 \equiv 1 \pmod 8$.*

For any odd prime p, an element $b \in \mathbb{Q}_p$ is a square if and only if it is of the form $b = p^n b_0$ with n an even integer and b_0 a quadratic residue modulo p.

Proof. $\Rightarrow$ For every p, if $b \in (\mathbb{Q}_p^\times)^2$, then $|b|_p \in 2\mathbb{Z}$, so $b = p^{2n} b_0$ with $b_0 \in (\mathbb{Z}_p^\times)^2$. If $b_0 = y_0^2$ for some $y_0 \in \mathbb{Z}_p^\times$, by expressing y_0 as $y_0 = \sum_{j=0}^{\infty} a_j p^j$ with $a_i \in \{0, \dots, p-1\}$, $a_0 \neq 0$ and squaring the series, it is easy to check that in the case where $p = 2$, we must have that $b_0 \equiv 1 \pmod 8$ and in the rest of the cases, $(\frac{b_0}{p}) = 1$.

$\Leftarrow$ If $b = p^{2m} b_0$, to prove that $b \in (\mathbb{Q}_p^\times)^2$ we must demonstrate that $b_0 \in (\mathbb{Q}_p^\times)^2$. To show this, we can apply Hensel's lemma on the polynomial $f(x) = x^2 - b_0$ with a correct choice of a_0.

- In the case $p = 2$, if $b_0 \equiv 1 \pmod 8$, we can consider $a_0 = 1$ and check that $|f(a_0)|_2 \leq 2^{-3}$ and $|f'(a_0)|_2^2 = 2^{-2}$, so there exists an $a \in \mathbb{Z}_2$ such that $a^2 = b_0$.
- Similarly, for any odd prime p, if $(\frac{b_0}{p}) = 1$ we can find an a_0 such that $a_0^2 \equiv b_0 \pmod p$, and we will have that $|f(a_0)| \leq p^{-1}$ and $|f'(a_0)|_2^2 = 1$. Thus, there exists an $a \in \mathbb{Z}_2$ such that $a^2 = b_0$. □

What this proposition tells us is that the group $\mathbb{Q}_p^\times/(\mathbb{Q}_p^\times)^2$ is generated by p and the generators of $\mathbb{Z}_p^\times/(\mathbb{Z}_p^\times)^2$. It can be checked that $\mathbb{Z}_2^\times/(\mathbb{Z}_2^\times)^2$ is isomorphic to the group of odd numbers modulo 8 ($\{\pm 1, \pm 5\}$) and for the odd primes $\mathbb{Z}_p^\times/(\mathbb{Z}_p^\times)^2$ only has a non-trivial element, corresponding to a quadratic non-residue of p. Therefore,

Corollary 2.1. *The group $\mathbb{Q}_2^\times/(\mathbb{Q}_2^\times)^2$ has order 8, so it is isomorphic to $(\mathbb{Z}/2\mathbb{Z})^3$ and may be represented by $\{\pm 1, \pm 2, \pm 5, \pm 10\}$.*

Let p be an odd prime. Then, $\mathbb{Q}_p^\times/(\mathbb{Q}_p^\times)^2$ has order 4 so it is isomorphic to $(\mathbb{Z}/2\mathbb{Z})^2$. A complete set of representatives is given by the set $\{1, p, c, cp\}$, where $c \in \mathbb{Z}_p^\times$ is an element whose reduction modulo p is not a quadratic residue.

A similar reasoning works for most local fields. In particular,

Proposition 2.4. *The group $\mathbb{Q}(i)_{1+i}^\times/(\mathbb{Q}(i)_{1+i}^\times)^2$ has order 16, so it is isomorphic to $(\mathbb{Z}/2\mathbb{Z})^4$ and it is generated by $\langle i, 1+2i, 2+i, 1+i\rangle$.*

Let $\mathfrak{p} \neq 1+i$ be a prime in $\mathbb{Z}[i]$. Then $\mathbb{Q}(i)_{\mathfrak{p}}^\times/(\mathbb{Q}(i)_{\mathfrak{p}}^\times)^2$ has order 4 and it is generated by $\langle \mathfrak{c}, \mathfrak{p}\rangle$, where $\mathfrak{c} \in \mathbb{Z}[i]_{1+i}^\times$ and $\mathfrak{c} \notin (\mathbb{Z}[i]_{1+i}^\times)^2$.

Proof. The proof is almost identical to the one in proposition 2.3. The only difficulty may be in the first statement, for which we first have to prove that $b \in \mathbb{Q}(i)_{1+i}$ if and only if $b = (1+i)^n b_0$ with n an even integer and

$$b_0 \equiv \pm 1 \pmod{(1+i)^5} \equiv \pm 1 \pmod{-4-4i}.$$

In order to check that $\#\mathbb{Q}(i)^\times_{1+i}/(\mathbb{Q}(i)^\times_{1+i})^2 = 16$, we could consider the group of elements in $\mathbb{Z}[i]/(1+i)^5\mathbb{Z}[i]$ that are not multiples of $(1+i)$, which will be denoted by $\mathbb{G}$. With a little of work, it can be proven that there is an epimorphism

$$\mu\colon \mathbb{G} \longrightarrow \mathbb{Z}[i]^\times_{1+i}/(\mathbb{Z}[i]^\times_{1+i})^2$$

with $\ker\mu = \{1,-1\}$. Then,

$$\#\mathbb{G} = \tfrac{1}{2}\,\#(\mathbb{Z}[i]/(1+i)^5\mathbb{Z}[i]) = \tfrac{1}{2}\,\mathrm{N}_{\mathbb{Q}(i)/\mathbb{Q}}(-4-4i) = 16,$$
$$\#(\mathbb{Z}[i]^\times_{1+i}/(\mathbb{Z}[i]^\times_{1+i})^2) = \#\mathbb{G}\,/\,\#\ker\mu = 8.$$

and therefore $\mathbb{Z}[i]^\times_{1+i}/(\mathbb{Z}[i]^\times_{1+i})^2$ has three generators, that can be chosen to be $i, 1+2i$ and $2+i$, so $\mathbb{Q}(i)^\times_{1+i}/(\mathbb{Q}(i)^\times_{1+i})^2 = \langle i, 1+2i, 2+i, 1+i\rangle$. □

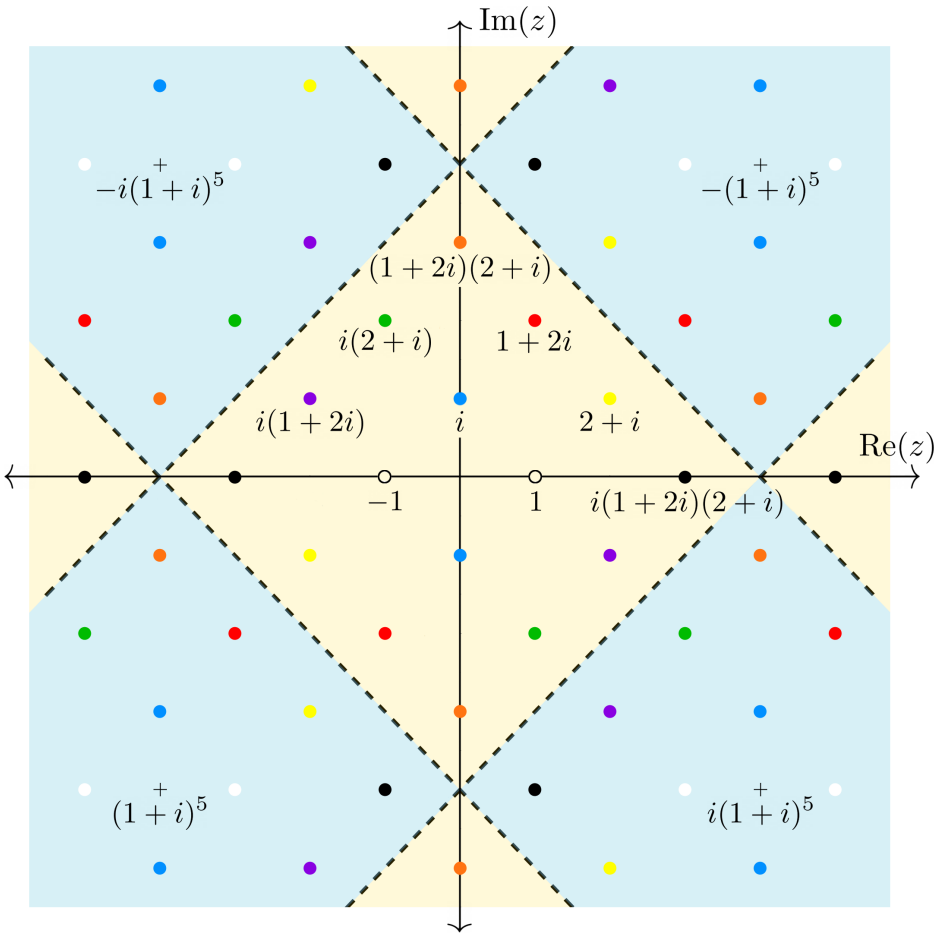

Figure 2.1: The dots represent the elements of $\mathbb{G}$ and their color shows their class of equivalence in $\mathbb{Z}[i]^\times_{1+i}/(\mathbb{Z}[i]^\times_{1+i})^2$. The regions in blue and orange represent the different domains of $\mathbb{Q}(i)$ modulo $(1+i)^5 = -4-4i$.

2.4 The Hasse principle

Both $\mathbb{R}$ and $\mathbb{Q}_p$ are fields that contain $\mathbb{Q}$ as a subfield, so no system of equations without a solution for either $\mathbb{R}$ or $\mathbb{Q}_p$ for some p prime, could possibly have a rational solution.

The **Hasse principle** asks about the inverse statement.

Definition 2.11 (Hasse principle). *If a system of polynomial equations with rational coefficients has a solution in $\mathbb{R}$ and in $\mathbb{Q}_p$ for every prime p, does it have a solution in $\mathbb{Q}$?*

This principle **does not hold in general**. We can easily produce equations on one variable that are counterexamples of it by using results of quadratic reciprocity.

Proposition 2.5. *Let p be an odd prime. Then,*

$$\begin{array}{lllll}
a) & \left(\frac{-1}{p}\right)=1 \iff p\equiv 1,-3 \pmod 8. & \left(\frac{-1}{p}\right)=-1 \iff p\equiv -1,\ \ 3 \pmod 8.\\
b) & \left(\frac{2}{p}\right)=1 \iff p\equiv 1,-1 \pmod 8. & \left(\frac{2}{p}\right)=-1 \iff p\equiv\ \ 3,-3 \pmod 8.\\
c) & \left(\frac{-2}{p}\right)=1 \iff p\equiv 1,\ \ 3 \pmod 8. & \left(\frac{-2}{p}\right)=-1 \iff p\equiv -1,-3 \pmod 8.\\
d) & \left(\frac{-3}{p}\right)=1 \iff p\equiv 1 \pmod 3. & \left(\frac{-3}{p}\right)=-1 \iff p\equiv -1 \pmod 3.
\end{array}$$

Proof. [Bro81, Section 3]. □

Hence,

Proposition 2.6. *Let q_1, q_2 be two distinct prime numbers such that $q_1 \equiv 1 \pmod 8$ and $\left(\frac{q_2}{q_1}\right)=1$. Then, the equation*

$$f(x)=(x^2-q_1)(x^2-q_2)(x^2-q_1q_2)=0$$

is a counterexample to the Hasse principle.[1]

Proof. It is easy to see that this equation has 6 real solutions $\{\pm\sqrt{q_1},\pm\sqrt{q_2},\pm\sqrt{q_1q_2}\}$ which are all irrational, as q_1 and q_2 are different primes.

The only thing left to see is that for every prime p, this equation has a solution in $\mathbb{Q}_p$. As $q_1 \equiv 1 \pmod 4$, from the law of quadratic reciprocity, $\left(\frac{q_1}{q_2}\right)=\left(\frac{q_1}{q_2}\right)=1$. From the corollary 2.3, we deduce that $q_1 \in (\mathbb{Q}_2^\times)^2$, $q_2 \in (\mathbb{Q}_{q_1}^\times)^2$ and $q_1 \in (\mathbb{Q}_{q_2}^\times)^2$, so $f(x)=0$ has solutions in $\mathbb{Q}_2$, $\mathbb{Q}_{q_1}$ and $\mathbb{Q}_{q_2}$.

For any other prime p different than $2, q_1, q_2$, we know that if $\left(\frac{q_1}{p}\right)=\left(\frac{q_2}{p}\right)=-1$, then

$$\left(\frac{q_1q_2}{p}\right)=\left(\frac{q_1}{p}\right)\left(\frac{q_2}{p}\right)=1.$$

Therefore, either q_1, q_2 or q_1q_2 must be a square in $\mathbb{Q}_p$ and so, the equation $f(x)=0$ has a solution in $\mathbb{Q}_p$ for every p prime. Hence, it is a counterexample to the Hasse principle. □

[1] This family is a generalisation of the typical example given in most references about local fields, which is $q_1=17$, $q_2=2$ [Cas86, Lemma 3]. All possible values $q_1, q_2 < 300$ can be found in table 4.7.

Despite failing in general, there are many cases where the Hasse principal holds. One of the most relevant ones is given by the **Hasse-Minkowski theorem**:

Theorem 2.3 (Hasse-Minkowski). *Let $f(X_1, X_2, \dots, X_n) = \sum_{i,j} c_{ij} X_i X_j$ with coefficients in $\mathbb{Q}$ be a quadratic form, i.e. a homogeneous polynomial of degree 2 on n variables. Then, the equation $f(X_1, X_2, \dots, X_n) = 0$ has non-trivial solutions in $\mathbb{Q}$ if and only if it has non-trivial solutions in $\mathbb{R}$ and $\mathbb{Q}_p$ for every p prime.*

Proof. [Ser73, Theorem 3.8]. □

This theorem shows that, from a geometrical point of view, there are limitations to finding counterexamples to the Hasse principle.

If we focus on studying the Hasse principle on **curves**[2] $\mathcal{C}$ over $\mathbb{Q}$, it can be proven that if the genus of $\mathcal{C}$ is 0, then $\mathcal{C}$ is $\mathbb{Q}$-birationally equivalent either to a line or to a conic section of the form $aX^2 + bY^2 + cZ^2 = 0$, with $a, b, c \in \mathbb{Q}$ [Cas67, Theorem 2.2]. This shows,

Theorem 2.4. *The Hasse principle holds for all curves of genus 0.*

It also implies that if we want to study and find counterexamples to the Hasse principle in curves, we will need to study curves of genus greater than 0.

The first counterexamples to the Hasse principle on curves were discovered while working with curves of genus 1:

Example 2.6 (**Lind and Reichart** [Lin40, Rei42]).

$$2Y^2 = Z^4 - 17X^4.$$

Example 2.7 (**Selmer** [Sel51]).

$$3X^3 + 4Y^3 + 5Z^3 = 0.$$

In the next chapter, we will explore the theory behind curves of genus 1 and how both local fields and the Hasse principle play a role in understanding their geometry.

[2] By curve over K, we mean a smooth, projective, irreducible, 1-dimensional K-variety.

3 The theory of elliptic curves

3.1 An introduction to elliptic curves

Definition 3.1. *An **elliptic curve** $\mathcal{E}$ over a field K is a non-singular curve of genus 1 with a K-rational point. We will write $\mathcal{E}/K$ to express that $\mathcal{E}$ is defined over K and we will denote by $\mathcal{E}(K)$ its set of K-rational points.*

One of the reasons why it is interesting to work with elliptic curves is because we can define a **group law** on their set of K-rational points that makes $\mathcal{E}(K)$ an abelian group [Cas91, Chapter 7]. By defining a homomorphism from $\mathcal{E}$ into $\mathbb{P}^2$ such that the neutral element of the group law gets mapped to the point of infinity $\underline{o} = [0 : 1 : 0]$, every elliptic curve is isomorphic to a curve given by the equation

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3$$

with $a_1, \ldots, a_6 \in K$. In affine coordinates $\{x = \frac{X}{Z}, y = \frac{Y}{Z}\}$, this equation is given by

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6. \tag{3.1}$$

in what it is known as the **Weierstrass equation** of $\mathcal{E}$. Moreover, if $\mathrm{char}(K) \neq 2, 3$, by completing the square every elliptic curve can be represented as $y^2 = x^3 + Ax^2 + B$ for some $A, B \in K$. On Connell's book [Con99, Chapter 1] it is described how to transform elliptic curves expressed as quartics, cubics and intersections of quadric surfaces into Weierstrass form.

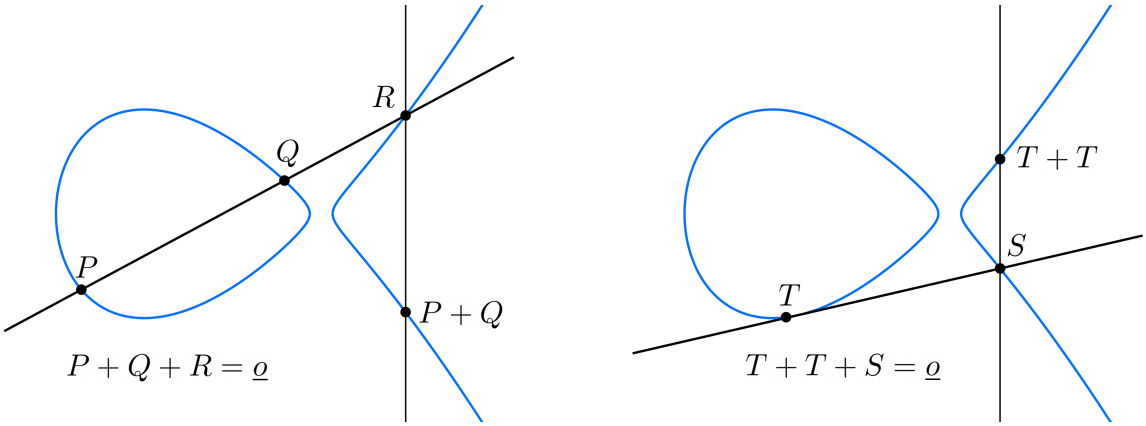

Figure 3.1: Group law (over $\mathbb{R}$) on the curve $y^2 = x(x-1)(x-\frac{97}{89})$.

Given a cubic curve in Weierstrass form, it is a non-singular curve if and only if its **discriminant** Δ is different to zero, where

$$\Delta = -b_2^2 b_8 - 8b_4^3 - 27b_6^2 + 9b_2 b_4 b_6 \quad \text{and} \tag{3.2}$$
$$\begin{cases} b_2 = a_1^2 + 4a_2, \\ b_4 = a_1 a_3 + 2a_4, \\ b_6 = a_3^2 + 4a_6, \\ b_8 = a_1^2 a_6 - a_1 a_3 a_4 + 4a_2 a_6 + a_2 a_3^2 - a_4^2. \end{cases}$$

When $\mathcal{E}$ is defined over a field K with some non-Archimedean $\mathfrak{p} \in M_K$, there will be a preferred representation of $\mathcal{E}$ by a Weierstrass equation.

Definition 3.2. *A Weierstrass equation for an elliptic curve $\mathcal{E}/K$ is called a **minimal Weierstrass equation** at $\mathfrak{p}$ if $v_\mathfrak{p}(\Delta)$ is minimized subject to the condition that $a_i \in R_K$.*

Finding minimal equations can be hard, but luckily, in the cases where K has class number 1, such as $K = \mathbb{Q}$ or $\mathbb{Q}(i)$, there exists a global Weierstrass equation defined over $\mathbb{Z}$ or $\mathbb{Z}[i]$ that is minimal at every non-Archimedean place $\mathfrak{p}$ [Sil09, Corollary 8.3]. Also, from a practical standpoint, if $0 \leq v_\mathfrak{p}(\Delta) < 12$ for a non-Archimedean place $\mathfrak{p}$ and $a_i \in R_K$, the equation is minimal at $\mathfrak{p}$ [Con99, Corollary 5.3.3].

This minimal equation will help us study elliptic curves defined over local fields $K_\mathfrak{p}$. If π is a uniformer for $R_{K_\mathfrak{p}}$, there is a natural reduction map:

$$\begin{aligned} R_{K_\mathfrak{p}} &\longrightarrow \kappa = R_{K_\mathfrak{p}}/\pi R_{K_\mathfrak{p}} \\ t &\longmapsto \bar{t} \end{aligned}$$

If we have a minimal Weierstrass equation for $\mathcal{E}/K_\mathfrak{p}$, we can reduce its coefficients to obtain a (possibly singular) curve $\bar{\mathcal{E}}$ defined over the residue field κ and called the **reduction** of $\mathcal{E}$ modulo π.

Now, if $P \in \mathcal{E}(K_\mathfrak{p})$, we can always express it in projective coordinates $P = [x, y, z]$ such that $x, y, z \in R_{K_\mathfrak{p}}$ and at least one of these coordinates is in $R_{K_\mathfrak{p}}^\times$. By defining the reduced point as $\bar{P} = [\bar{x}, \bar{y}, \bar{z}] \in \bar{\mathcal{E}}(\kappa)$, this defines a **reduction map**:

$$\begin{aligned} \mathcal{E}(K_\mathfrak{p}) &\longrightarrow \bar{\mathcal{E}}(\kappa) \\ P &\longmapsto \bar{P} \end{aligned}$$

Definition 3.3. *Let $\mathcal{E}$ an elliptic curve over K, a number field with a non-Archimedean absolute value $|\ |_\mathfrak{p}$ and completion $K_\mathfrak{p}$. Let $\bar{\mathcal{E}}$ be the reduction of a minimal Weierstrass equation of $\mathcal{E}$ at $\mathfrak{p}$. We say that $\mathcal{E}$ has **bad reduction** at $\mathfrak{p}$ if and only if $\bar{\mathcal{E}}$ is singular.*

It can easily be seen that a minimal Weierstrass equation $\mathcal{E}$ has bad reduction at $\mathfrak{p}$ if and only if $v_\mathfrak{p}(\Delta) > 0$ [Sil09, Proposition 5.1]. The reduction map plays a very important role in understanding elliptic curves, as in all the places where $\mathcal{E}$ does not have bad reduction, we can obtain information about $\mathcal{E}$ from $\bar{\mathcal{E}}$, which is an elliptic curve defined over a finite field, therefore easier to analyse.

There are some key definitions in the theory of elliptic curves

Definition 3.4. *Let $\mathcal{E}_1/K$ and $\mathcal{E}_2/K$ be elliptic curves. An **isogeny** on $\mathcal{E}_1(K)$ is a morphism $\phi\colon \mathcal{E}_1(K) \longrightarrow \mathcal{E}_2(K)$ satisfying $\phi(\underline{o}) = \underline{o}$.*

Definition 3.5. *For each $m \in \mathbb{N}$ the **multiplication-by-m isogeny** on $\mathcal{E}(K)$ is*

$$\begin{aligned}[m]\colon\ \mathcal{E}(K) &\longrightarrow \mathcal{E}(K)\\ P &\longmapsto \underbrace{P + \cdots + P}_{m \text{ terms}}.\end{aligned}$$

Definition 3.6. *Let $m \in \mathbb{Z}$ with $m \geq 2$. The **m-torsion subgroup** of $\mathcal{E}(K)$ is*

$$\mathcal{E}(K)[m] = \{P \in \mathcal{E}(K) : [m]P = \underline{o}\}.$$

We will denote by $\mathcal{E}_{\text{tors}}(K)$ the points of finite order in $\mathcal{E}$, i.e.,

$$\mathcal{E}_{\text{tors}}(K) = \bigcup_{m=2}^{\infty} \mathcal{E}(K)[m].$$

It is important to have in mind is that if $\mathcal{E}$ is given by an affine Weierstrass equation (3.1) with $a_1 = a_3 = 0$ and $P = (x_P, y_P) \in \mathcal{E}(K)$, then $-P = (x_P, -y_P)$ and

$$P \in \mathcal{E}(K)[2] \iff [2]P = \underline{o} \iff P = -P \iff y_P = 0.$$

Therefore, $P \in \mathcal{E}(K)[2]$ if and only if $P = \underline{o}$ or $P = (x_i, 0)$ with $x_i \in K$ and

$$x_i^3 + a_2 x_i^2 + a_4 x_i + a_6 = 0.$$

Computing $\mathcal{E}_{\text{tors}}(K)$ is not as easy as computing $\mathcal{E}(K)[2]$ but it is feasible for some number fields K, as there are theorems [Con99, Section 2.10] that put limitations on the possible coordinates of torsion points in $\mathcal{E}(K)$. In the case of $\mathcal{E}(\mathbb{Q})$, these are given by a theorem known as **Nagell-Lutz theorem** [Con99, Proposition 2.10.4].

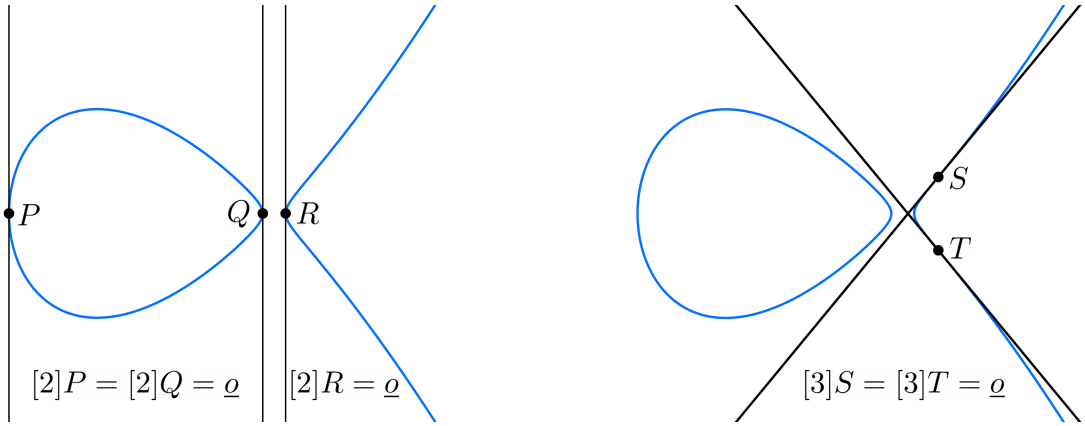

Figure 3.2: $\mathcal{E}(\mathbb{R})[2]$ and $\mathcal{E}(\mathbb{R})[3]$ for $\mathcal{E} : y^2 = x(x-1)(x-\frac{97}{89})$.

3.2 The Mordell-Weil theorem

From now on, K will be a **number field**. Then, the structure of the group of K-rational points of an elliptic curve is given by the following theorem:

Theorem 3.1 (Mordell-Weil). *Let $\mathcal{E}/K$ be an elliptic curve. Then the group $\mathcal{E}(K)$ is finitely generated.*

The fundamental theorem of finitely generated abelian groups implies that

$$\mathcal{E}(K) \cong \mathcal{E}_{\text{tors}}(K) \times \mathbb{Z}^r, \tag{3.3}$$

where $\mathcal{E}_{\text{tors}}(K)$ is finite, and r is called the **rank** of $\mathcal{E}(K)$.

Computing the rank of an elliptic curve is generally a very difficult task, even when we restrict ourselves to the case where $K = \mathbb{Q}$, as we will see in chapter 4. In fact, it is still unknown whether there exist elliptic curves over $\mathbb{Q}$ with **arbitrarily large rank**.

The Mordell-Weil theorem is usually proved from a **weaker version** by the means of the so-called **height functions**, which give a notion of "size" on the points of $\mathcal{E}(K)$ [PSZ03, Chapter 5].

Theorem 3.2 (Weak Mordell-Weil). *Let $\mathcal{E}/K$ be an elliptic curve and let $m \geq 2$ be an integer. Then $\mathcal{E}(K)/m\,\mathcal{E}(K)$ is a finite group.*

It is easy to see that that the Mordell-Weil theorem implies its weaker version, as by (3.3),

$$\mathcal{E}(K)/m\mathcal{E}(K) \cong \mathcal{E}_{\text{tors}}(K)/m\mathcal{E}_{\text{tors}}(K) \times (\mathbb{Z}/m\mathbb{Z})^r$$

and in the case where $m = 2$, it becomes

$$\mathcal{E}(K)/2\,\mathcal{E}(K) \cong \mathcal{E}(K)[2] \times (\mathbb{Z}/2\mathbb{Z})^r. \tag{3.4}$$

A full proof of theorem 3.2 theorem can be found in Silverman's book [Sil09, Theorem VIII.1.1]. We will now provide an intuition about why this result is true and how it relates to the geometry of an elliptic curve through its cohomology.

3.2.1 A crash course on Galois cohomology

Explaining the theory behind the Galois cohomology of a curve in full detail would go well-beyond the scope of this dissertation. The purpose of the following sections is to explain the main results of this theory and how they relate to explicit computations. For a more detailed approach to cohomology, one can check the book by Harari [Har20].

Let K be a number field, and let $\bar{K}$ be the algebraic closure of K. Then, the **(absolute) Galois group** of $\bar{K}/K$, which we will denote by $G_{\bar{K}/K}$ is

$$G_{\bar{K}/K} = \text{Gal}(\bar{K}/K) = \varprojlim_{L/K \text{ finite Galois}} \text{Gal}(L/K).$$

$G_{\bar{K}/K}$ is what is known as a **profinite group**, an inverse limit of finite groups.
It comes equipped with a topology in which a basis of open sets consists of the collection of normal subgroups having finite index in $G_{\bar{K}/K}$, which are all kernels of maps $G_{\bar{K}/K} \to \mathrm{Gal}(L/K)$ for finite Galois extensions L/K [Sil09, Section B.2].

Definition 3.7. *A $\boldsymbol{G_{\bar{K}/K}}$-module is an abelian group A such that the action of $G_{\bar{K}/K}$ on A is continuous with respect to the profinite topology on $G_{\bar{K}/K}$ and the discrete topology in A.*

Definition 3.8. *The $\mathbf{0^{th}}$ cohomology group of the $G_{\bar{K}/K}$-module A is the group of $G_{\bar{K}/K}$-invariant elements of A:*

$$H^0(G_{\bar{K}/K}, A) = \{a \in A \colon a^\sigma = a \text{ for all } \sigma \in G_{\bar{K}/K}\}.$$

By considering the profinite topology in $G_{\bar{K}/K}$ and the discrete one in A, we can focus on the continuous maps $\xi \colon G_{\bar{K}/K} \to A$ to give the following definitions:

Definition 3.9. *The group of continuous 1-cocycles from $G_{\bar{K}/K}$ to A is the group*

$$Z^1_{\mathrm{cont}}(G_{\bar{K}/K}, A) = \{\xi \text{ continuous} : \xi_{\sigma\tau} = \xi_\sigma^\tau + \xi_\tau \text{ for all } \sigma, \tau \in G_{\bar{K}/K}\}.$$

Definition 3.10. *The group of 1-coboundaries from $G_{\bar{K}/K}$ to A is the group*

$$B^1(G_{\bar{K}/K}, A) = \{\xi \colon \text{ there exists an } a \in A \text{ such that } \xi_\sigma = a^\sigma - a \text{ for all } \sigma \in A\}.$$

Since A has the discrete topology, every coboundary is automatically continuous, so it is easy to check that $B^1(G_{\bar{K}/K}, A)$ is a subgroup (and in fact, a normal subgroup) of $Z^1_{\mathrm{cont}}(G_{\bar{K}/K}, A)$. Then,

Definition 3.11. *The $\mathbf{1^{st}}$ cohomology group of the $G_{\bar{K}/K}$-module A is the group*

$$H^1(G_{\bar{K}/K}, A) = Z^1_{\mathrm{cont}}(G_{\bar{K}/K}, A) \,/\, B^1(G_{\bar{K}/K}, A).$$

We are interested in cohomology because $G_{\bar{K}/K}$ acts on the points of $\mathcal{E}(\bar{K})$ by

$$\sigma(\underline{o}) = \underline{o} \qquad\qquad \sigma(x_P, y_P) = (\sigma(x_P), \sigma(y_P)),$$

where $P = (x_P, y_P) \in \mathcal{E}(\bar{K})$ and $\sigma \in G_{\bar{K}/K}$.

Every non-zero isogeny ϕ induces an exact sequence of $G_{\bar{K}/K}$- modules of the form

$$0 \longrightarrow \mathcal{E}(\bar{K})[\phi] \longrightarrow \mathcal{E}(\bar{K}) \xrightarrow{\phi} \mathcal{E}'(\bar{K}) \longrightarrow 0,$$

where $\mathcal{E}(\bar{K})[\phi] = \ker \phi$.

That sequence can be extended [Har20, Theorem 1.17] to a sequence between cohomology groups

$$0 \longrightarrow H^0(G_{\bar{K}/K}, \mathcal{E}(\bar{K})[\phi]) \xrightarrow{i} H^0(G_{\bar{K}/K}, \mathcal{E}(\bar{K})) \xrightarrow{\phi} H^0(G_{\bar{K}/K}, \mathcal{E}'(\bar{K})) \xrightarrow{\delta} H^1(G_{\bar{K}/K}, \mathcal{E}(\bar{K})[\phi]) \longrightarrow H^1(G_{\bar{K}/K}, \mathcal{E}(\bar{K})) \xrightarrow{\phi} H^1(G_{\bar{K}/K}, \mathcal{E}'(\bar{K})).$$

and, from the definition of the 0^{th} cohomology group, we get:

$$0 \longrightarrow \mathcal{E}(K)[\phi] \longrightarrow \mathcal{E}(K) \xrightarrow{\phi} \mathcal{E}'(K) \xrightarrow{\delta} H^1(G_{\bar{K}/K}, \mathcal{E}(\bar{K})[\phi]) \longrightarrow H^1(G_{\bar{K}/K}, \mathcal{E}(\bar{K})) \xrightarrow{\phi} H^1(G_{\bar{K}/K}, \mathcal{E}'(\bar{K})).$$

Furthermore, from this sequence we can deduce the fundamental exact short sequence

$$0 \longrightarrow \mathcal{E}'(K)/\phi(\mathcal{E}(K)) \xrightarrow{\delta} H^1(G_{\bar{K}/K}, \mathcal{E}(\bar{K})[\phi]) \longrightarrow H^1(G_{\bar{K}/K}, \mathcal{E}(\bar{K}))[\phi] \longrightarrow 0. \tag{3.5}$$

3.3 Descent in elliptic curves

From the discussion of the Mordell-Weil theorem, it seems natural to study $\mathcal{E}(K)$ by analysing $\mathcal{E}(K)/m\mathcal{E}(K)$ for some $m \in \mathbb{Z}$. To do so, we can consider the multiplication-by-m isogeny, which gives us

$$0 \longrightarrow \mathcal{E}(K)/m\mathcal{E}(K) \xrightarrow{\delta} H^1(G_{\bar{K}/K}, \mathcal{E}(\bar{K})[m]) \xrightarrow{\psi} H^1(G_{\bar{K}/K}, \mathcal{E}(\bar{K}))[m] \longrightarrow 0.$$

As δ is an injective morphism, studying $\mathcal{E}(K)/m\mathcal{E}(K)$ is equivalent to studying $\operatorname{im}\delta$, which is equal to $\ker\psi$. We will see that there is an interpretation of $H^1(G_{\bar{K}/K}, \mathcal{E}(\bar{K}))$ that will help us to understand the elements of the kernel of ψ in a practical way.

3.3.1 The Weil-Châtelet group

Definition 3.12. *Let $\mathcal{E}/K$ be an elliptic curve. A **homogeneous space** for $\mathcal{E}$ is a pair $(\mathcal{C}, +_{\mathcal{C}})$, where $\mathcal{C}$ is a smooth curve over K and*

$$+_{\mathcal{C}} : \mathcal{C} \times \mathcal{E} \longrightarrow \mathcal{C}$$

is a morphism defined over K satisfying

1. *$p +_{\mathcal{C}} \underline{o} = p$ for all $p \in \mathcal{C}$.*
2. *$(p +_{\mathcal{C}} P) + Q = p +_{\mathcal{C}} (P + Q)$ for all $p \in \mathcal{C}$ and $P, Q \in \mathcal{E}$.*
3. *For all $p, q \in \mathcal{C}$, there is a unique $P \in \mathcal{E}$ satisfying $p +_{\mathcal{C}} P = q$*

A careful analysis of these spaces $\mathcal{C}/K$ shows that they are all isomorphic to $\mathcal{E}/K$ over $\bar{K}$ [Sil09, Proposition X.3.2]. Furthermore, we can define an equivalence relation in the set of all homogeneous spaces of $\mathcal{E}/K$ by considering two homogeneous spaces $\mathcal{C}_1/K$ and $\mathcal{C}_2/K$ to be **equivalent** if there is an isomorphism $\theta : \mathcal{C}_1 \to \mathcal{C}_2$ defined over K such that

$$\theta(p +_{\mathcal{C}_1} P) = \theta(p) +_{\mathcal{C}_2} P$$

for all $p \in \mathcal{C}_1$ and all $P \in \mathcal{E}$. Then,

Definition 3.13. *The set of equivalence classes of homogeneous spaces for $\mathcal{E}/K$ forms a group*[3] *that is called the **Weil-Châtelet group** of $\mathcal{E}$ and denoted by $\mathrm{WC}(\mathcal{E}/K)$.*

The reason why the Weil-Châtelet group is interesting is because it is **isomorphic** to $H^1(G_{\bar{K}/K}, \mathcal{E}(K))$ [Sil09, Theorem X.3.6]. The advantage of working with $\mathrm{WC}(\mathcal{E}/K)$ over $H^1(G_{\bar{K}/K}, \mathcal{E}(K))$ is that the elements of $\mathrm{WC}(\mathcal{E}/K)$ which belong to the **trivial class** can be found through the following criterion:

Proposition 3.1. *Let $\mathcal{C}/K$ be a homogeneous space for $\mathcal{E}$. Then $\mathcal{C}$ is the trivial class if and only if $\mathcal{C}(K)$ is not the empty set.*

Proof. [Sil09, Proposition X.3.3]. □

Under the identification of $H^1(G_{\bar{K}/K}, \mathcal{E}(K))$ and $\mathrm{WC}(\mathcal{E}/K)$, we get an intuition for the elements of $\mathcal{E}(K)/m\mathcal{E}(K)$. As they can be identified with the elements of $\ker \psi$, we can see them as the elements of $H^1(G_{\bar{K}/K}, \mathcal{E}(\bar{K})[m])$ which get sent to homogeneous spaces that have solutions in K.

3.3.2 Complete 2-descent

In the case where $\mathcal{E}$ is given by an equation $y^2 = f(x)$ where all the roots of $f(x)$ are in K, $H^1(G_{\bar{K}/K}, \mathcal{E}(\bar{K})[2])$ can be identified with a subgroup of $K^\times/(K^\times)^2$ and the elements of $\mathcal{E}(K)/2\mathcal{E}(K)$ can be explicitly computed from the solutions over K of homogeneous spaces. This gives us a method to study the rank of a curve known as **complete 2-descent**.

Theorem 3.3 (Complete 2-descent). *Let $\mathcal{E}$ be an elliptic curve over a field K given by a Weierstrass equation of the form $y^2 = (x-a)(x-b)(x-c)$ with $a, b, c \in K$.*

Let $S \subset M_K$ be a finite set of places of K including all Archimedean places, all places dividing 2, and all places at which $\mathcal{E}$ has bad reduction. Furthermore, let

$$K(S,2) = \{s \in K^\times/(K^\times)^2 : v_\mathfrak{p}(s) \equiv 0 \pmod 2 \text{ for all } \mathfrak{p} \notin S\}.$$

Then, there is an injective morphism $\mu\colon \mathcal{E}(K)/2\mathcal{E}(K) \to K(S,2) \times K(S,2)$ defined by

$$P = (x_P, y_P) \longmapsto \mu(P) = \begin{cases} [1,1] & \text{if } P = \underline{o} \\ [\frac{a-c}{a-b}, a-b] & \text{if } x_P = a \\ [b-a, \frac{b-c}{b-a}] & \text{if } x_P = b \\ [x_P - a, x_P - b] & \text{if } x_P \neq a, b \end{cases}$$

[3] An explicit construction of the group law can be found in Weil's article [Wei55, Proposition 5].

Let $[s_1, s_2] \in K(S,2) \times K(S,2)$ be a pair that is not the image of one of the three points $\{\underline{o}, (a,0), (b,0)\}$. Then $[s_1, s_2]$ is the image of a point $P = (x_P, y_P) \in \mathcal{E}(K)/2\mathcal{E}(K)$ if and only if the system

$$\begin{cases} s_1 x^2 \ - \ s_2 y^2 \ = b - a \\ s_1 x^2 - s_1 s_2 z^2 = c - a \end{cases} \tag{3.6}$$

has a solution $(x, y, z) \in K^\times \times K^\times \times K$. If such a solution exists, then we can take

$$P = (x_P, y_P) = (s_1 x^2 + a, \ s_1 s_2 \, a \, b \, c).$$

Proof. [Sil09, Proposition X.1.4]. □

This result gives us a way of explicitly compute $\mathrm{rank}_{\mathbb{Z}/2\mathbb{Z}} \mathcal{E}(K)/2\mathcal{E}(K)$ given that we are able to determine the existence or non-existence of K-rational points in the homogeneous spaces.

In section 2.3 we saw that through Hensel's lemma, computing points in local fields is easier than in their global counterparts. Hence, a natural approach to study the K-points of the homogeneous spaces would be to consider the local fields $K_\mathfrak{p}$ of K and find solutions in those fields. In the next section, we will follow this approach.

3.4 The Selmer and Tate-Shafarevich groups

We recall (3.5) that, for every isogeny ϕ

$$0 \longrightarrow \mathcal{E}'(K)/\phi(\mathcal{E}(K)) \xrightarrow{\delta} H^1(G_{\bar{K}/K}, \mathcal{E}(\bar{K})[\phi]) \longrightarrow \mathrm{WC}(\mathcal{E}/K)[\phi] \longrightarrow 0.$$

For each $\mathfrak{p} \in M_K$ we fix an extension of $\mathfrak{p}$ in $\bar{K}$, which serves to fix an embedding of $\bar{K}_\mathfrak{p}$ and a decomposition group $G_\mathfrak{p}$ (a subgroup $G_\mathfrak{p} \leq G_{\bar{K}/K}$ fixing $\mathfrak{p}$) in such a way that $G_\mathfrak{p}$ acts on $\mathcal{E}(\bar{K}_\mathfrak{p})$ and $\mathcal{E}'(\bar{K}_\mathfrak{p})$ [Sil09, Section X.4]. By the same argument as before,

$$0 \longrightarrow \mathcal{E}'(K_\mathfrak{p})/\phi(\mathcal{E}(K_\mathfrak{p})) \xrightarrow{\delta} H^1(G_\mathfrak{p}, \mathcal{E}(\bar{K}_\mathfrak{p})[\phi]) \longrightarrow \mathrm{WC}(\mathcal{E}/K_\mathfrak{p})[\phi] \longrightarrow 0. \tag{3.7}$$

It can be proven [Har20, Section 1.5] that the maps $G_\mathfrak{p} \hookrightarrow G_{\bar{K}/K}$ and $\mathcal{E}(\bar{K}) \hookrightarrow \mathcal{E}(\bar{K}_\mathfrak{p})$ induce maps between the cohomology groups, known as **restriction maps**, such that we can construct the diagram:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathcal{E}'(K)/\phi(\mathcal{E}(K)) & \xrightarrow{\delta} & H^1(G_{\bar{K}/K}, \mathcal{E}(\bar{K})[\phi]) & \longrightarrow & \mathrm{WC}(\mathcal{E}/K)[\phi] & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & \prod_{\mathfrak{p}\in M_K} \mathcal{E}'(K)/\phi(\mathcal{E}(K)) & \xrightarrow{\delta} & \prod_{\mathfrak{p}\in M_K} H^1(G_\mathfrak{p}, \mathcal{E}(\bar{K}_\mathfrak{p})[\phi]) & \longrightarrow & \prod_{\mathfrak{p}\in M_K} \mathrm{WC}(\mathcal{E}/K_\mathfrak{p})[\phi] & \longrightarrow & 0 \end{array}$$

Then we can define:

Definition 3.14. *The ϕ-**Selmer group** of $\mathcal{E}/K$ is the group*

$$\mathrm{Sel}^{(\phi)}(\mathcal{E}/K) = \ker\left\{H^1(G_{\bar{K}/K}, \mathcal{E}(\bar{K})[\phi]) \to \prod_{\mathfrak{p}\in M_K} \mathrm{WC}(\mathcal{E}/K_\mathfrak{p})\right\}.$$

Definition 3.15. *The **Tate-Shafarevich group** of $\mathcal{E}/K$ is the group*

$$Ш(\mathcal{E}/K) = \ker\left\{\mathrm{WC}(\mathcal{E}/K) \to \prod_{\mathfrak{p}\in M_K} \mathrm{WC}(\mathcal{E}/K_\mathfrak{p})\right\}.$$

Even though the sequence (3.7) depended on the extension of $\mathfrak{p}$ that we considered, it can be easily checked that the definitions 3.14 and 3.15 do not depend on anything but $\mathcal{E}$ and K [Sil09, Remark X.4.1.1]. From our previous diagrams, we deduce that there is an exact sequence

$$0 \longrightarrow \mathcal{E}'(K)/\phi(\mathcal{E}(K)) \longrightarrow \mathrm{Sel}^{(\phi)}(\mathcal{E}/K) \longrightarrow Ш(\mathcal{E}/K)[\phi] \longrightarrow 0.$$

where $\mathrm{Sel}^{(\phi)}(\mathcal{E}/K)$ is always finite [Cas67, Section 23].

From our interpretation of the Weil-Châtelet group, we can see that the ϕ-Selmer group consists of the elements of $H^1(G_{\bar{K}/K}, \mathcal{E}(\bar{K})[\phi])$ that get sent to homogeneous spaces that have solutions in every completion $K_\mathfrak{p}$ of K.

Thus, $\mathrm{Sel}^{(\phi)}(\mathcal{E}/K)$ gives us a bound of the rank of $\mathcal{E}(K)/\phi(\mathcal{E}(K))$. When we are under the hypothesis of complete 2-descent, i.e. $\phi = [2]$ and $\mathcal{E}(\bar{K})[2] \subset \mathcal{E}(K)$, we get

$$0 \longrightarrow \mathcal{E}(K)/2\mathcal{E}(K) \longrightarrow \mathrm{Sel}^{(2)}(\mathcal{E}/K) \longrightarrow Ш(\mathcal{E}/K)[2] \longrightarrow 0.$$

and so

$$\begin{aligned}\mathrm{rank}_{\mathbb{Z}/2\mathbb{Z}}\,\mathrm{Sel}^{(2)}(\mathcal{E}/K) &= \mathrm{rank}_{\mathbb{Z}/2\mathbb{Z}}\,\mathcal{E}(K)/2\mathcal{E}(K) + \mathrm{rank}_{\mathbb{Z}/2\mathbb{Z}}\,Ш(\mathcal{E}/K)[2] \\ &= 2 + \mathrm{rank}_{\mathbb{Z}}\,\mathcal{E}(K) + \mathrm{rank}_{\mathbb{Z}/2\mathbb{Z}}\,Ш(\mathcal{E}/K)[2], \qquad (3.8)\end{aligned}$$

as $\mathrm{rank}_{\mathbb{Z}/2\mathbb{Z}}\,\mathcal{E}(K)[2] = 2$.

While the ϕ-Selmer group has an easy interpretation, the Tate-Shafarevich group of $\mathcal{E}/K$ is a more mysterious group. It can be interpreted as the classes of homogeneous spaces that have $K_\mathfrak{p}$-rational points for every $\mathfrak{p} \in M_K$, but no K-rational points. Hence, in the case where $K = \mathbb{Q}$, the elements of $Ш(\mathcal{E}/\mathbb{Q})$ can be thought as the classes of homogeneous spaces that **do not satisfy the Hasse principle**.

In order to find counterexamples to the Hasse principle, a good approach is to search for curves $\mathcal{E}/\mathbb{Q}$ with non-trivial $Ш(\mathcal{E}/\mathbb{Q})$. If we are able to find the homogeneous spaces that correspond to elements in $\mathrm{Sel}^{(\phi)}(\mathcal{E}/\mathbb{Q})$ but do not correspond to elements in $\mathcal{E}'(\mathbb{Q})/\phi(\mathcal{E}(\mathbb{Q}))$, those spaces would correspond to non-trivial elements in $Ш(\mathcal{E}/\mathbb{Q})[\phi]$.

That is the method that we will use in chapter 4 to construct a counterexample, and it is also what is behind the example 2.6, as the affine version of the curve, $2y^2 = 1 - 17x^4$ appears as an homogeneous space of $Ш(\mathcal{E}/\mathbb{Q})[\phi]$, for

$$\mathcal{E} : y^2 = x^3 + 17x, \qquad \mathcal{E}' : v^2 = u^3 - 68u,$$

and

$$\begin{aligned} \phi : \mathcal{E} &\longrightarrow \mathcal{E}' \\ (x, y) &\longmapsto (u, v) = \left(\frac{y^2}{x^2}, \frac{y(17 - x^2)}{x^2}\right). \end{aligned}$$

The Tate-Shafarevich group plays a role in many conjectures about elliptic curves, including the famous **Birch and Swinnerton-Dyer conjecture** [PSZ03, Conjecture 7.17]. Among those conjectures, a very relevant one for this dissertation is that **the Tate-Shaferevich group of an elliptic curve is always finite**.

In relation to the order of $Ш(\mathcal{E}/K)$, Cassels proved [Cas62, Theorem 1.1] that if $Ш(\mathcal{E}/K)$ is finite, $\#Ш(\mathcal{E}/K)$ is a square. The same is true for the order of any of the p-primary components of $Ш(\mathcal{E}/K)$ so, in particular, if $Ш(\mathcal{E}/K)$ is finite, $\#Ш(\mathcal{E}/K)[2]$ is a square and

$$\operatorname{rank}_{\mathbb{Z}/2\mathbb{Z}} Ш(\mathcal{E}/K)[2] \equiv 0 \pmod 2.$$

Therefore, by 3.8

Proposition 3.2. *If $Ш(\mathcal{E}/K)$ is finite,*

$$\operatorname{rank}_{\mathbb{Z}/2\mathbb{Z}} \operatorname{Sel}^{(2)}(\mathcal{E}/K) \equiv \operatorname{rank}_{\mathbb{Z}} \mathcal{E}(K) \pmod 2.$$

3.5 An alternative way of performing 2-descent

Let $\mathcal{E}/K$ with $\mathcal{E}(\bar{K})[2] \subset \mathcal{E}(K)$. As we saw before, complete 2-descent 3.3 gave us a way to compute $\mathcal{E}(K)/2\mathcal{E}(K)$ and $\operatorname{Sel}^{(2)}(\mathcal{E}/K)$ by translating the problem into finding solutions in K and $K_\mathfrak{p}$ of systems of equations (3.6). This method works well in concrete examples where we can use a computer to find those solutions. However, if our intention is to study a general family of curves, working with the homogeneous spaces can be complicated. After all, the theorem 3.3 implies that if $\#S = m$ then $\#K(S, 2) = 2^m$, and we would need to study the solutions of 2^{2m} systems of equations.

We will now present an alternative way to perform 2-descent. This approach has been described in the book of Cassels and Flynn [CF96, Chapter 11] and applied to the study of elliptic curves and the Jacobian of curves of genus 2 in articles by Flynn [FR03, Fly18]. Using this method, we avoid having to work explicitly with the homogeneous spaces by simplifying the problem of computing $\operatorname{Sel}^{(2)}(\mathcal{E}/K)$ into finding generators of the groups $\mathcal{E}(K_\mathfrak{p})/2\mathcal{E}(K_\mathfrak{p})$.

Let $K_\mathfrak{p}$ be a local field of K and let M be a finite subset of $K(S,2)\times K(S,2)$ containing the image of the map μ defined in theorem 3.3. Then, μ induces a commutative diagram

$$\begin{array}{ccc} \mathcal{E}(K)/2\mathcal{E}(K) & \xrightarrow{\mu} & M \\ \downarrow{\scriptstyle i_\mathfrak{p}} & & \downarrow{\scriptstyle j_\mathfrak{p}} \\ \mathcal{E}(K_\mathfrak{p})/2\mathcal{E}(K_\mathfrak{p}) & \xrightarrow{\mu_\mathfrak{p}} & M_{K_\mathfrak{p}} \end{array}$$

where $\mu_\mathfrak{p}$ is defined as in theorem 3.3, but over $K_\mathfrak{p}$ instead of K, and the maps $i_\mathfrak{p}$ and $j_\mathfrak{p}$ are natural maps on the quotient induced by the inclusion map from K to $K_\mathfrak{p}$.

Suppose that we want to study which homogeneous spaces associated to elements of M have solutions in $K_\mathfrak{p}$. By searching points in $\mathcal{E}(K_\mathfrak{p})$, we can find a complete set of generators for $\mathcal{E}(K_\mathfrak{p})/2\mathcal{E}(K_\mathfrak{p})$ and through these elements we can compute $\operatorname{im}\mu_\mathfrak{p}$. Because the diagram is commutative, $j_\mathfrak{p}^{-1}(\operatorname{im}\mu_\mathfrak{p})$ must contain $\operatorname{im}\mu$, and by considering $M\cap j_\mathfrak{p}^{-1}(\operatorname{im}\mu_\mathfrak{p})$, we have managed to find a subset of M whose elements represent homogeneous spaces that have solutions in $K_\mathfrak{p}$.

By computing the intersection of $j_\mathfrak{p}^{-1}(\operatorname{im}\mu_\mathfrak{p})$ for every place $\mathfrak{p}\in M_K$, we end up finding the elements of $K(S,2)\times K(S,2)$ that have solution in every local field of K, thus, the 2-Selmer group of $\mathcal{E}/K$. Moreover, Milne proved [Mil86, Corollary 6.6] that, in fact, we only need to compute $j_\mathfrak{p}^{-1}(\operatorname{im}\mu_\mathfrak{p})$ for $\mathfrak{p}\in S$ as,

$$\operatorname{Sel}^{(2)}(\mathcal{E}/K)=\bigcap_{\mathfrak{p}\in S} j_\mathfrak{p}^{-1}(\operatorname{im}\mu_\mathfrak{p}).$$

3.5.1 The order of $\mathcal{E}(K_\mathfrak{p})/2\mathcal{E}(K_\mathfrak{p})$

From the description of the method, it may not be apparent why searching for a set of generators for $\mathcal{E}(K_\mathfrak{p})/2\mathcal{E}(K_\mathfrak{p})$ will be easier than searching one for $\mathcal{E}(K)/2\mathcal{E}(K)$. The main two reasons are that we can use Hensel's lemma to construct points in $\mathcal{E}(K_\mathfrak{p})$ and that the order of $\mathcal{E}(K_\mathfrak{p})/2\mathcal{E}(K_\mathfrak{p})$ is given by the following result:

Theorem 3.4. *Let $\mathcal{E}$ be an elliptic curve defined over $K_\mathfrak{p}$, a completion of a number field by a non-Archimedean valuation. Then, $\mathcal{E}(K_\mathfrak{p})$ contains a subgroup $\mathcal{H}$ of finite index that is isomorphic to the additive group of $\mathcal{M}_{K_\mathfrak{p}}$, the valuation ideal of $K_\mathfrak{p}$, and*

$$\#\mathcal{E}(K_\mathfrak{p})/2\mathcal{E}(K_\mathfrak{p})=\#\mathcal{E}(K_\mathfrak{p})[2]\cdot\#\mathcal{M}_{K_\mathfrak{p}}/2\mathcal{M}_{K_\mathfrak{p}}.$$

Proof. [CF96, Theorem 7.5.1]. □

From this theorem, we can deduce the following results:

Proposition 3.3. *Let $\mathcal{E}/\mathbb{Q}$ and let p be an odd prime. Then,*

$$\begin{aligned}\#\mathcal{E}(\mathbb{R})/2\mathcal{E}(\mathbb{R}) &= \tfrac{1}{2}\#\mathcal{E}(\mathbb{R})[2],\\ \#\mathcal{E}(\mathbb{Q}_2)/2\mathcal{E}(\mathbb{Q}_2) &= 2\,\#\mathcal{E}(\mathbb{Q}_2)[2],\\ \#\mathcal{E}(\mathbb{Q}_p)/2\mathcal{E}(\mathbb{Q}_p) &= \#\mathcal{E}(\mathbb{Q}_p)[2].\end{aligned}$$

Proof. For the cases where the local field is $\mathbb{Q}_p$, we can apply proposition 2.1. If p is odd, $|2|_p = 1$ and so, $2 \in \mathbb{Z}_p^\times$. Thus, $2\mathcal{M}_{\mathbb{Q}_p} = \mathcal{M}_{\mathbb{Q}_p}$ and so, $\#\mathcal{M}_{\mathbb{Q}_p}/2\mathcal{M}_{\mathbb{Q}_p} = 1$. However, when $\mathcal{M}_{\mathbb{Q}_2} = 2\mathbb{Z}_2$, 2 is not a unit of $\mathbb{Z}_2$ and we see that $2\mathcal{M}_{\mathbb{Q}_2} = 4\mathbb{Z}_2$ is a proper subgroup of $\mathcal{M}_{\mathbb{Q}_2}$ and $\#\mathcal{M}_{\mathbb{Q}_2}/2\mathcal{M}_{\mathbb{Q}_2} = \#2\mathbb{Z}_2/4\mathbb{Z}_2 = 2$.

The proof for the case $\mathcal{E}(\mathbb{R})/2\mathcal{E}(\mathbb{R})$ is more subtle and can be found in the book by Cassels and Flynn [CF96, Section 7.6]. □

Proposition 3.4. *Let $\mathcal{E}/\mathbb{Q}(i)$ and $\mathfrak{p}$ a prime different from $1+i$. Then,*

$$\begin{aligned}\#\mathcal{E}(\mathbb{C})/2\mathcal{E}(\mathbb{C}) &= 1,\\ \#\mathcal{E}(\mathbb{Q}(i)_{1+i})/2\mathcal{E}(\mathbb{Q}(i)_{1+i}) &= 4\,\#\mathcal{E}(\mathbb{Q}(i)_{1+i})[2],\\ \#\mathcal{E}(\mathbb{Q}(i)_{\mathfrak{p}})/2\mathcal{E}(\mathbb{Q}(i)_{\mathfrak{p}}) &= \#\mathcal{E}(\mathbb{Q}(i)_{\mathfrak{p}})[2].\end{aligned}$$

Proof. It can easily be checked that if $P = (x, y(x))$, $[2]P = (\phi(x), y(\phi(x))$ for some rational function $\phi(x)$. As $\mathbb{C}$ is algebraically closed, the equation $x_0 = \phi(x)$ has solutions for every x_0 in $\mathbb{C}$, so $[2]$ is a surjective map and $\mathcal{E}(\mathbb{C})/2\mathcal{E}(\mathbb{C})$ is trivial.

For the case of $\mathbb{Q}(i)_{1+i}$, we have that $\mathcal{M}_{\mathbb{Q}(i)_{1+i}} = (1+i)\mathbb{Z}[i]_{1+i}$ and, as 2 is not a unit of $\mathcal{M}_{\mathbb{Q}(i)_{1+i}}$, we have the proper subgroup

$$2\mathcal{M}_{\mathbb{Q}(i)_{1+i}} = 2(1+i)\mathbb{Z}[i]_{1+i} = (1+i)^3\mathbb{Z}[i]_{1+i}$$

and so, it satisfies that $\#\mathcal{M}_{\mathbb{Q}(i)_{1+i}}/2\mathcal{M}_{\mathbb{Q}(i)_{1+i}} = \#(1+i)\mathbb{Z}[i]_{1+i}/(1+i)^3\mathbb{Z}[i]_{1+i} = 2^2 = 4$. Finally, for the rest of primes, $\#\mathcal{M}_{\mathbb{Q}(i)_{1+i}}/2\mathcal{M}_{\mathbb{Q}(i)_{1+i}} = 1$ as $|2|_{\mathfrak{p}} = 1$. □

3.5.2 Quadratic twists

While the method that we have described to perform 2-descent is very effective to compute the 2-Selmer group, it is not particularly helpful to compute the rank of a curve, as it only gives us an upper bound (as $\operatorname{rank}_{\mathbb{Z}/2\mathbb{Z}} \mathcal{E}(K)/2\mathcal{E}(K) \leq \operatorname{rank}_{\mathbb{Z}/2\mathbb{Z}} \operatorname{Sel}^{(2)}(\mathcal{E}/\mathbb{Q})$). However, we will see that by studying a curve related to $\mathcal{E}$, we will be able to get information about $\operatorname{rank}_{\mathbb{Z}} \mathcal{E}(K)$.

Definition 3.16. *Let $\mathcal{E}/K$ given by a Weierstrass equation*

$$y^2 = x^3 + a_2x^2 + a_4x + a_6$$

*and let $d \in K^\times$ an element that is not a square in K. Then, the **quadratic twist** of $\mathcal{E}$ with respect to d is the curve $\mathcal{E}_d/K$ defined as*

$$\mathcal{E}_d\colon y^2 = x^3 + da_2x^2 + d^2a_4x + d^3a_6.$$

Theorem 3.5. *Let $\mathcal{E}/K$ be an elliptic curve and let $\mathcal{E}_d$ its quadratic twist. Then,*

$$\operatorname{rank}_{\mathbb{Z}} \mathcal{E}(K(\sqrt{d})) = \operatorname{rank}_{\mathbb{Z}} \mathcal{E}(K) + \operatorname{rank}_{\mathbb{Z}} \mathcal{E}_d(K).$$

Proof. The proof for the more general case of n-twists can be found in the book by Pethö, Schmitt and Zimmer [PSZ03, Theorem 7.34]. □

We will now see some applications of the theory just discussed.

4 Construction of counterexamples to the Hasse principle

As per the introduction, one of the goals of this dissertation is to present an original counterexample to the Hasse principle. After analysing a family of curves, I have been able to isolate the values which generate such counterexamples.

Theorem 4.1. *Let p be a prime such that*

1. *$p+8$ is also prime.*
2. *$p \equiv p+8 \equiv 1 \pmod 8$.*
3. *$\left(\frac{2}{p}\right)_4 = -\left(\frac{2}{p+8}\right)_4$ i.e. 2 is a quartic residue of either p or $p+8$ but it is not a quartic residue of both of them.*

Then, the elliptic curve defined as

$$\mathcal{E} : y^2 = x(x-p)(x-p-8) \tag{4.1}$$

satisfies that $\operatorname{rank}_{\mathbb{Z}}(\mathcal{E}(\mathbb{Q})) = 0$ and $Ш(\mathcal{E}/\mathbb{Q})[2] = (\mathbb{Z}/2\mathbb{Z})^2$, provided that $Ш(\mathcal{E}/\mathbb{Q})$ is finite.

As seen in the previous chapter, this result about the geometry of $\mathcal{E}$ translates in the following characterisation of its homogeneous spaces through complete 2-descent:

Theorem 4.2. *Let p be as before. Then,*

$$\begin{aligned} \mu(\mathcal{E}(\mathbb{Q})/2\mathcal{E}(\mathbb{Q})) &= \langle [p,-2p],[p+8,2]\rangle, \\ \operatorname{Sel}^{(2)}(\mathcal{E}/\mathbb{Q}) &= \langle [1,-1],[1,2],[p,-2p],[p+8,2]\rangle, \end{aligned}$$

with $\mu(\mathcal{E}(\mathbb{Q})/2\mathcal{E}(\mathbb{Q})), \operatorname{Sel}^{(2)}(\mathcal{E}/\mathbb{Q}) \subset \mathbb{Q}^\times/(\mathbb{Q}^\times)^2 \times \mathbb{Q}^\times/(\mathbb{Q}^\times)^2$.

Thus, if $[s_1,s_2] \in \operatorname{Sel}^{(2)}(\mathcal{E}/\mathbb{Q}) \setminus \mu(\mathcal{E}(\mathbb{Q})/2\mathcal{E}(\mathbb{Q}))$, the system of equations

$$\begin{cases} s_1x^2 - s_2y^2 = p \\ s_1x^2 - s_1s_2z^2 = p+8 \end{cases} \tag{4.2}$$

has solutions in every completion of $\mathbb{Q}$ but does not have a rational solution.

The first thing that must be checked is that there exists primes p satisfying the conditions of the theorem 4.1. This is indeed the case, with $p = 89$ being the smallest possible value.

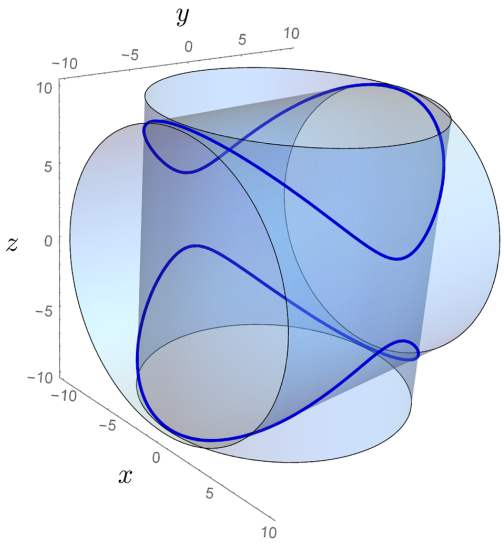

Figure 4.1: Graph of equation 4.2 for $p = 89, \quad [s_1, s_2] = [1, -1]$.

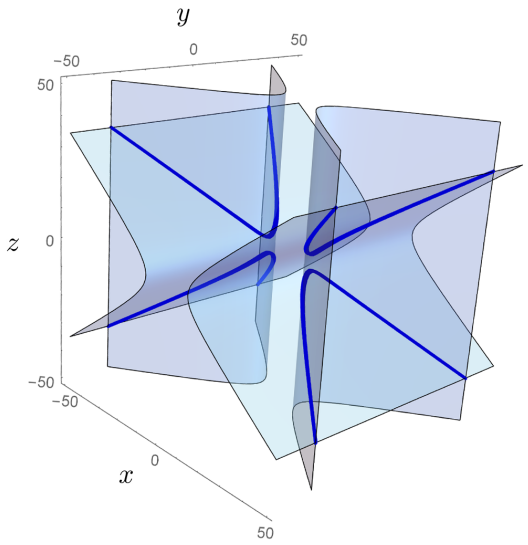

Figure 4.2: Graph of equation 4.2 for $p = 89, \quad [s_1, s_2] = [1, 2]$.

A list with all the possible values of p such that $p <$100 000 can be found in table A.2.

4.1 Outline of the proof

The way theorem 4.1 will be proven is by following these steps:

- First, using the technique described in section 3.5, we will prove that

$$\mathrm{Sel}^{(2)}(\mathcal{E}/\mathbb{Q}) = \langle [1,-1], [1,2], [p,-2p], [p+8,2] \rangle$$

  and so, $\mathrm{rank}_{\mathbb{Z}/2\mathbb{Z}}\, \mathrm{Sel}^{(2)}(\mathcal{E}/\mathbb{Q}) = 4$.

- Then, using the same technique we will prove that the rank of the 2-Selmer group over $\mathbb{Q}$ of $\mathcal{E}_{-1}$, the quadratic twist by -1, is 3. As $\mathrm{rank}_{\mathbb{Z}/2\mathbb{Z}}\, \mathcal{E}_{-1}(\mathbb{Q})[2] = 2$ and the 2-Selmer group and the rank have the same parity (proposition 3.2), this shows that $\mathrm{rank}_{\mathbb{Z}}(\mathcal{E}_{-1}(\mathbb{Q})) = 1$.

- Finally, we will prove that $\mathrm{rank}_{\mathbb{Z}/2\mathbb{Z}}\, \mathrm{Sel}^{(2)}(\mathcal{E}/\mathbb{Q}(i)) = 3$. This forces the rank of $\mathcal{E}(\mathbb{Q}(i))$ to be 1, and by the theorem 3.5, this implies that the rank of $\mathcal{E}(\mathbb{Q})$ is 0. Hence, by (3.8),

$$\mathrm{rank}_{\mathbb{Z}/2\mathbb{Z}}\, Ш(\mathcal{E}/\mathbb{Q})[2] = \mathrm{rank}_{\mathbb{Z}/2\mathbb{Z}}\, \mathrm{Sel}^{(2)}(\mathcal{E}/\mathbb{Q}) - \mathrm{rank}_{\mathbb{Z}}\, \mathcal{E}(\mathbb{Q}) - 2 = 2.$$

Before proving the result, we will demonstrate some properties of p.

Proposition 4.1. *Let p as in theorem 4.1. Then:*

a) *3 is not a quadratic residue modulo p, but it is a quadratic residue modulo $p+8$.*

b) *There exists an element $n \in \mathbb{Z}$ such that $\left(\frac{n}{p+8}\right) = -1$ and $\left(\frac{n+8}{p+8}\right) = 1$.*

Proof. *a)* As $p + 8 - p \equiv 2 \pmod 3$ and p and $p+8$ are primes, the only possibility is that $p \equiv -1 \pmod 3$ and $p + 8 \equiv 1 \pmod 3$. By proposition 2.5, we deduce that $\left(\frac{-3}{p}\right) = -\left(\frac{-3}{p+8}\right) = -1$, so the result follows since $\left(\frac{-1}{p}\right) = \left(\frac{-1}{p+8}\right) = 1$.

b) From *a)* and the proposition 2.5, we deduce that all the integers in the interval $[-4, 4]$ are quadratic residues modulo $p+8$. If there were no $n \in \mathbb{Z}$ such that $\left(\frac{n}{p+8}\right) = -1$ and $\left(\frac{n+8}{p+8}\right) = 1$, then we would deduce that all integers in $[-12, -4]$ would have to be quadratic residues modulo $p + 8$. By repeating this reasoning, we would prove that all integers in $(-\infty, 4]$, thus all integers modulo $p + 8$ are quadratic residues, which would lead to a contradiction. □

4.2 The 2-Selmer group of $\mathcal{E}$ over $\mathbb{Q}$

From equation 3.2, we deduce that the discriminant of $\mathcal{E}$ is

$$\Delta = 2^{10}\, p^2\, (p+8)^2.$$

As $v_{\mathfrak{p}}(\Delta) < 12$ for all $\mathfrak{p} \in M_{\mathbb{Q}}$, from section 3.1, we deduce that the equation 4.1 is minimal and the set of all places at which $\mathcal{E}$ has bad reduction is $\{2,\ p,\ p+8\}$. Hence,

$$S = \{\infty,\ 2,\ p,\ p+8\} \qquad \text{and} \qquad \mathbb{Q}(S,2) = \langle -1,\ 2,\ p,\ p+8\rangle,$$

and so,

$$\mathbb{Q}(S,2) \times \mathbb{Q}(S,2) = \langle [1,-1],\ [1,2],\ [1,p],\ [1,p+8],\ [-1,1],\ [2,1],\ [p,1],\ [p+8,1]\rangle.$$

The 2-torsion points of $\mathcal{E}$ are $\{(0,0), (p,0), (p+8,0)\}$, so $\mathcal{E}(\mathbb{Q})[2] \cong (\mathbb{Z}/2\mathbb{Z})^2$ and there is a map μ between $\mathcal{E}(\mathbb{Q})/2\mathcal{E}(\mathbb{Q})$ and $\mathbb{Q}(S,2) \times \mathbb{Q}(S,2)$:

$$P = (x_P, y_P) \longmapsto \mu(P) = \begin{cases} [1,1] & \text{if } P = \underline{o} \\ [p(p+8), -p] & \text{if } x_P = 0 \\ [p, -2p] & \text{if } x_P = p \\ [x_P, x_P - p] & \text{if } x_P \neq 0,\ p \end{cases}$$

In particular, $(p+8, 0) \overset{\mu}{\mapsto} [p+8, 2]$, and $\mu(\mathcal{E}(\mathbb{Q})[2]/2\mathcal{E}(\mathbb{Q})) = \langle [p, -2p],\ [p+8, 2]\rangle$.

4.2.1 Restriction to $\mathbb{R}$

Let us start by considering $M_0 = \mathbb{Q}(S,2) \times \mathbb{Q}(S,2)$. We get the diagram:

$$\begin{array}{ccc} \mathcal{E}(\mathbb{Q})/2\mathcal{E}(\mathbb{Q}) & \xrightarrow{\mu} & M_0 \\ \downarrow{\scriptstyle i_\infty} & & \downarrow{\scriptstyle j_\infty} \\ \mathcal{E}(\mathbb{R})/2\mathcal{E}(\mathbb{R}) & \xrightarrow{\mu_\infty} & (M_0)_{\mathbb{R}} \end{array}$$

In order to study μ_∞ and $(M_0)_{\mathbb{R}}$, it is important to notice that $\mathbb{R}^\times/(\mathbb{R}^\times)^2 = \{1,-1\}$, as either a number or its opposite is a square in $\mathbb{R}$. By proposition 3.3, $\#\mathcal{E}(\mathbb{R})/2\mathcal{E}(\mathbb{R}) = 2$, and it is easy to check that $(p,0) \overset{\mu_\infty}{\longmapsto} [p,-2p] = [1,-1]$. As μ_∞ is injective, and the image of $(p,0)$ is not $[1,1]$, we deduce that $(p,0) \neq \underline{o}$ in $\mathcal{E}(\mathbb{R})/2\mathcal{E}(\mathbb{R})$, and

$$\mathcal{E}(\mathbb{R})/2\mathcal{E}(\mathbb{R}) = \langle (p,0) \rangle, \qquad \operatorname{im} \mu_\infty = \langle [1,-1] \rangle.$$

The images of the generators of M_0 under the map j_∞ are as follows:

$$\begin{array}{cccccccc} [1,-1] & [1,2] & [1,p] & [1,p+8] & [-1,1] & [2,1] & [p,1] & [p+8,1] \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ [1,-1] & [1,1] & [1,1] & [1,1] & [-1,1] & [1,1] & [1,1] & [1,1] \end{array}$$

All the generators of M_0 except of $[-1,1]$ go to the image of μ_∞ in $(M_0)_{\mathbb{R}}$ through the map j_∞. As any product of $[-1,1]$ with any other element of M_0 except of itself go to either $[-1,1]$ or $[-1,-1]$, which do not belong to $\operatorname{im} \mu_\infty$, we deduce that

$$M_1 \coloneqq M_0 \cap j_\infty^{-1}(\operatorname{im} \mu_\infty) = \langle [1,-1],\ [1,2],\ [1,p],\ [1,p+8],\ [2,1],\ [p,1],\ [p+8,1] \rangle.$$

4.2.2 Restriction to $\mathbb{Q}_2$

We now check which homogeneous spaces associated to M_1 do not have solutions in $\mathbb{Q}_2$. To do so, we consider the diagram:

$$\begin{array}{ccc} \mathcal{E}(\mathbb{Q})/2\mathcal{E}(\mathbb{Q}) & \xrightarrow{\mu} & M_1 \\ \downarrow{\scriptstyle i_2} & & \downarrow{\scriptstyle j_2} \\ \mathcal{E}(\mathbb{Q}_2)/2\mathcal{E}(\mathbb{Q}_2) & \xrightarrow{\mu_2} & (M_1)_{\mathbb{Q}_2} \end{array}$$

We proved in corollary 2.1 that $\mathbb{Q}_2^\times/(\mathbb{Q}_2^\times)^2$ had 8 elements and a set of representatives was $\{\pm 1, \pm 2, \pm 5, \pm 10\}$. From proposition 3.3, we know that $\#\mathcal{E}(\mathbb{Q}_2)/2\mathcal{E}(\mathbb{Q}_2) = 8$, so it is generated by 3 elements. As $p \equiv p+8 \equiv 1 \pmod 8$, we deduce that $p = p+8 = 1$ in $\mathbb{Q}_2^\times/(\mathbb{Q}_2^\times)^2$.

Thus, the images of the 2-torsion points of $\mathcal{E}(\mathbb{Q})$ under μ_2 are:

$$(0,0) \overset{\mu_2}{\longmapsto} [1,-1], \qquad (p,0) \overset{\mu_2}{\longmapsto} [1,-2], \qquad (p+8,0) \overset{\mu_2}{\longmapsto} [1,2].$$

As $[1,-1]$ and $[1,2]$ are independent in $\mathbb{Q}_2^\times/(\mathbb{Q}_2^\times)^2 \times \mathbb{Q}_2^\times/(\mathbb{Q}_2^\times)^2$, we deduce that $(0,0)$ and $(p+8,0)$ are two generators of $\mathcal{E}(\mathbb{Q}_2)/2\mathcal{E}(\mathbb{Q}_2)$. We still need to find another generator of $\mathcal{E}(\mathbb{Q}_2)/2\mathcal{E}(\mathbb{Q}_2)$ in order to completely know $\operatorname{im}\mu_2$. That generator can be computed by constructing a point of $\mathcal{E}(\mathbb{Q}_2)/2\mathcal{E}(\mathbb{Q}_2)$ in the following way.

Proposition 4.2. *Let $m \in \mathbb{Z}$ such that $m \equiv p \pmod{32}$, and ϵ_m be a square root of $(p-m+4)(-m+4)(-m-4)$ in $\mathbb{Q}_2$. Then the point $(p-m+4, \epsilon_m)$ is a point of $\mathcal{E}(\mathbb{Q}_2)/2\mathcal{E}(\mathbb{Q}_2)$ that is not included in $\langle (0,0), (p+8,0)\rangle$.*

Proof. We first have to check that this point is well-defined. From the definition of m, $p-m+4 \equiv 4 \pmod{32}$, so $p-m+4$ is divisible by 4 but not by 8, and

$$\tfrac{1}{4}(p-m+4) \equiv 1 \pmod{8}.$$

Also, as $m \equiv 1 \pmod{8}$, $-m+4$ and $-m-4$ are both odd numbers and

$$(-m+4)(-m-4) \equiv m^2 - 16 \equiv 1 \pmod{8}.$$

Hence, $\epsilon_m^2 = 4\,\frac{1}{4}(p-m+4)(-m+4)(-m-4)$ is the product of 4 by an odd number that is congruent to 1 modulo 8, and by proposition 2.3, ϵ_m is defined in $\mathbb{Q}_2$.

To see that this point is independent of $(0,0)$ and $(p+8,0)$, it suffices to see that $(p-m+4, \epsilon_m) \overset{\mu_2}{\longmapsto} [p-m+4, -m+4] = [1,-5]$, which is not in $\langle [1,-1], [1,2]\rangle$. □

From this proposition, we deduce that

$$\mathcal{E}(\mathbb{Q}_2)/2\mathcal{E}(\mathbb{Q}_2) = \langle (0,0), (p+8,0), (p-m+4, \epsilon_m)\rangle,$$
$$\operatorname{im}\mu_2 = \langle [1,-1], [1,2], [1,-5]\rangle.$$

The images of the generators of M_1 under j_2 are:

$$\begin{array}{ccccccc} [1,-1] & [1,2] & [1,p] & [1,p+8] & [2,1] & [p,1] & [p+8,1] \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ [1,-1] & [1,2] & [1,1] & [1,1] & [2,1] & [1,1] & [1,1] \end{array}$$

As all generators go to elements of $\operatorname{im}\mu_2$ except for $[2,1]$, and every product of $[2,1]$ with any other different element does not belong to $\operatorname{im}\mu_2$, we deduce that

$$M_2 := M_1 \cap j_2^{-1}(\operatorname{im}\mu_2) = \langle [1,-1],\ [1,2],\ [1,p],\ [1,p+8],\ [-1,1],\ [p,1],\ [p+8,1]\rangle.$$

4.2.3 Restriction to $\mathbb{Q}_p$

Considering the place p, we have:

$$\begin{array}{ccc} \mathcal{E}(\mathbb{Q})/2\mathcal{E}(\mathbb{Q}) & \xrightarrow{\mu} & M_2 \\ \downarrow{\scriptstyle i_p} & & \downarrow{\scriptstyle j_p} \\ \mathcal{E}(\mathbb{Q}_p)/2\mathcal{E}(\mathbb{Q}_p) & \xrightarrow{\mu_p} & (M_2)_{\mathbb{Q}_p} \end{array}$$

Corollary 2.1 implies that $\mathbb{Q}_p^\times/(\mathbb{Q}_p^\times)^2$ has order 4. Moreover, as 3 is not a quadratic residue modulo p (proposition 4.1), we know that a set of representatives is given by $\{1, 3, p, 3p\}$, and it is generated by 2 elements since $\#\mathcal{E}(\mathbb{Q}_p)/2\mathcal{E}(\mathbb{Q}_p) = 4$.

From the proposition 2.5, we deduce that $-1, 2, -2$ and $p+8$ are all equivalent to 1 in $\mathbb{Q}_p^\times/(\mathbb{Q}_p^\times)^2$. Therefore,

$$(0,0) \overset{\mu_p}{\longmapsto} [p,p], \qquad (p,0) \overset{\mu_p}{\longmapsto} [p,p], \qquad (p+8,0) \overset{\mu_p}{\longmapsto} [1,1],$$

so $(0,0)$ is one of the generators of $\mathcal{E}(\mathbb{Q}_p)/2\mathcal{E}(\mathbb{Q}_p)$. For the other generator, we can consider the point $(p+6, \alpha)$ where α is the square root of $(p+6)\,6\,(-2)$ in $\mathbb{Q}_p^\times/(\mathbb{Q}_p^\times)^2$.

This root exists as $\left(\frac{6}{p}\right) = -1$, $\left(\frac{p+6}{p}\right) = -1$ and $\left(\frac{(p+6)\,6\,(-2)}{p}\right) = 1$, thus

$$(p+6)\,6\,(-2) \in (\mathbb{Q}_p^\times)^2.$$

Hence, $(p+6, \alpha) \overset{\mu_p}{\longmapsto} [3,3]$ and

$$\mathcal{E}(\mathbb{Q}_p)/2\mathcal{E}(\mathbb{Q}_p) = \langle (0,0), (p+6,\alpha)\rangle, \qquad \operatorname{im}\mu_p = \langle [p,p], [3,3]\rangle.$$

Under j_p the images of the generators of M_2 are:

$$\begin{array}{cccccc} [1,-1] & [1,2] & [1,p] & [1,p+8] & [p,1] & [p+8,1] \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ [1,1] & [1,1] & [1,p] & [1,1] & [p,1] & [1,1] \end{array}$$

All generators go to the identity under j_p, except for $[1,p]$ and $[p,1]$. However, as their product goes to $[p,p] \in \operatorname{im}\mu_p$, we deduce that

$$M_3 := M_2 \cap j_p^{-1}(\operatorname{im}\mu_p) = \langle [1,-1],\ [1,2],\ [1,p+8],\ [-1,1],\ [p+8,1],\ [p,p]\rangle.$$

4.2.4 Restriction to $\mathbb{Q}_{p+8}$

In this last case,

$$\begin{array}{ccc} \mathcal{E}(\mathbb{Q})/2\mathcal{E}(\mathbb{Q}) & \xrightarrow{\quad\mu\quad} & M_3 \\ \downarrow{\scriptstyle i_{p+8}} & & \downarrow{\scriptstyle j_{p+8}} \\ \mathcal{E}(\mathbb{Q}_{p+8})/2\mathcal{E}(\mathbb{Q}_{p+8}) & \xrightarrow{\mu_{p+8}} & (M_3)_{\mathbb{Q}_{p+8}} \end{array}$$

As in the previous case, $\#\mathbb{Q}_{p+8}^{\times}/(\mathbb{Q}_{p+8}^{\times})^2 = 4$. A complete set of representatives is given by $\{1, n, p+8, n(p+8)\}$ where n is as in proposition 4.1, that is, $(\frac{n}{p+8}) = -1$ and $(\frac{n+8}{p+8}) = 1$. As before, $\mathcal{E}(\mathbb{Q}_{p+8})/2\mathcal{E}(\mathbb{Q}_{p+8})$ is generated by 2 elements. From proposition 2.5, we deduce that $-1, 2, -2$ and p are all equivalent to 1 in $\mathbb{Q}_{p+8}^{\times}/(\mathbb{Q}_{p+8}^{\times})^2$. Hence,

$$(0,0) \xmapsto{\mu_{p+8}} [p+8,1], \qquad (p,0) \xmapsto{\mu_{p+8}} [1,1], \qquad (p+8,0) \xmapsto{\mu_{p+8}} [p+8,1].$$

Therefore, $(0,0)$ is one of the generators of $\mathcal{E}(\mathbb{Q}_{p+8})/2\mathcal{E}(\mathbb{Q}_{p+8})$. Another generator is the point $(p+8+n, \beta_n)$ where β_n is the square root of $(p+8+n)(n+8)n$. We then have that $(p+8+n, \beta_n) \xmapsto{\mu_{p+8}} [n,1]$ and so,

$$\mathcal{E}(\mathbb{Q}_{p+8})/2\mathcal{E}(\mathbb{Q}_{p+8}) = \langle (0,0), (p+8+n, \beta_n) \rangle, \qquad \operatorname{im}\mu_{p+8} = \langle [p+8,1], [n,1] \rangle.$$

The images of the generators of M_3 under j_{p+8} are:

$$\begin{array}{ccccc} [1,-1] & [1,2] & [1,p+8] & [p+8,1] & [p,p] \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ [1,1] & [1,1] & [1,p+8] & [p+8,1] & [1,1] \end{array}$$

As all elements except for $[1,p+8]$ and its products with other generators go to $\operatorname{im}\mu_{p+8}$,

$$\begin{aligned} \langle [1,-1],\ [1,2],\ [p+8,1],\ [p,p] \rangle &= M_3 \cap j_{p+8}^{-1}(\operatorname{im}\mu_{p+8}) \\ &= M_2 \cap j_p^{-1}(\operatorname{im}\mu_p) \cap j_{p+8}^{-1}(\operatorname{im}\mu_{p+8}) \\ &= M_1 \cap j_2^{-1}(\operatorname{im}\mu_2) \cap j_p^{-1}(\operatorname{im}\mu_p) \cap j_{p+8}^{-1}(\operatorname{im}\mu_{p+8}) \\ &= \bigcap_{\mathfrak{p}\in S} j_{\mathfrak{p}}^{-1}(\operatorname{im}\mu_{\mathfrak{p}}) \\ &= \mathrm{Sel}^{(2)}(\mathcal{E}/\mathbb{Q}) \end{aligned}$$

By reordering the generators and using that

$$[p,-2p] = [p,p] * [1,-1] * [1,2] \qquad [p+8,2] = [p+8,1] * [1,2],$$

it is easy to check that $\mathrm{Sel}^{(2)}(\mathcal{E}/\mathbb{Q}) = \langle [1,-1], [1,2], [p,-2p], [p+8,2] \rangle$, where

$$\mu(\mathcal{E}(\mathbb{Q})[2]/2\mathcal{E}(\mathbb{Q})) = \langle [p,-2p],\ [p+8,2] \rangle.$$

4.3 The 2-Selmer group of $\mathcal{E}_{-1}$ over $\mathbb{Q}$

Given the elliptic curve $\mathcal{E}$, its quadratic twist by the element -1 is given by the equation

$$\mathcal{E}_{-1}\colon y^2 = x(x+p)(x+p+8).$$

As it also has three rational 2-torsion points, we can apply the same technique to find its rank. The discriminant of $\mathcal{E}_{-1}$ is $\Delta = 2^{10}\,p^2\,(p+8)^2$, so the set of all places at which $\mathcal{E}$ has bad reduction is, once again, $\{2,\ p,\ p+8\}$. Therefore,

$$\mathbb{Q}(S,2)\times\mathbb{Q}(S,2) = \langle [1,-1],\ [1,2],\ [1,p],\ [1,p+8],\ [-1,1],\ [2,1],\ [p,1],\ [p+8,1]\rangle.$$

This time the 2-torsion points of $\mathcal{E}_{-1}$ are $\{(0,0),(-p,0),(-p-8,0)\}$, so the map μ between $\mathcal{E}_{-1}(\mathbb{Q})/2\mathcal{E}_{-1}(\mathbb{Q})$ and $\mathbb{Q}(S,2)\times\mathbb{Q}(S,2)$ is as follows:

$$P=(x_P,y_P)\ \longmapsto\ \mu(P) = \begin{cases} [1,1] & \text{if } P=\underline{o}\\ [p(p+8),p] & \text{if } x_P=0\\ [-p,-2p] & \text{if } x_P=-p\\ [x_P,x_P+p] & \text{if } x_P\neq 0,\ -p\end{cases}$$

Thus, $(-p-8,0)\overset{\mu}{\mapsto}[-p-8,-2]$, and

$$\mu(\mathcal{E}_{-1}(\mathbb{Q})[2]/2\mathcal{E}_{-1}(\mathbb{Q})) = \langle [-p,-2p],\ [-p-8,-2]\rangle.$$

By considering $m\in\mathbb{Z}$ and $a\in\mathbb{Z}$ as before, and defining $\epsilon_m,\delta_m,\alpha$ and β_n appropriately,

$$\begin{aligned}
\mathcal{E}_{-1}(\mathbb{R})/2\mathcal{E}_{-1}(\mathbb{R}) &= \langle(-p,0)\rangle,\\
\operatorname{im}\mu_\infty &= \langle[-1,-1]\rangle,\\
\mathcal{E}_{-1}(\mathbb{Q}_2)/2\mathcal{E}_{-1}(\mathbb{Q}_2) &= \langle(-p,0),\ (-p+m+4,\epsilon_m),\ (-p+m+5,\delta_m)\rangle,\\
\operatorname{im}\mu_2 &= \langle[-1,-2],\ [1,5],\ [5,-10]\rangle,\\
\mathcal{E}_{-1}(\mathbb{Q}_p)/2\mathcal{E}_{-1}(\mathbb{Q}_p) &= \langle(0,0),(-p-6,\alpha)\rangle,\\
\operatorname{im}\mu_p &= \langle[p,p],\ [3,3]\rangle,\\
\mathcal{E}_{-1}(\mathbb{Q}_{p+8})/2\mathcal{E}_{-1}(\mathbb{Q}_{p+8}) &= \langle(0,0),(p+8+n,\beta_n)\rangle,\\
\operatorname{im}\mu_{p+8} &= \langle[p+8,1],[n,1]\rangle.
\end{aligned}$$

By setting $M_0 \coloneqq \mathbb{Q}(S,2)\times\mathbb{Q}(S,2)$, we then have

$$\begin{aligned}
M_1 &\coloneqq M_0\cap j_\infty^{-1}(\operatorname{im}\mu_\infty) = \langle[1,2],\ [1,p],\ [1,p+8],\ [2,1],\ [p,1],\ [p+8,1],\ [-1,-1]\rangle,\\
M_2 &\coloneqq M_1\cap j_2^{-1}(\operatorname{im}\mu_2) = \langle[1,p],\ [1,p+8],\ [p,1],\ [p+8,1],\ [-1,-2]\rangle,\\
M_3 &\coloneqq M_2\cap j_p^{-1}(\operatorname{im}\mu_p) = \langle[1,p+8],\ [p+8,1],\ [-1,-2],\ [p,p]\rangle,
\end{aligned}$$

and after computing $M_3\cap j_{p+8}^{-1}(\operatorname{im}\mu_{p+8})$, we get

$$\begin{aligned}
\operatorname{Sel}^{(2)}(\mathcal{E}_{-1},\mathbb{Q}) &= \bigcap_{\mathfrak{p}\in S} j_{\mathfrak{p}}^{-1}(\operatorname{im}\mu_{\mathfrak{p}})\\
&= \langle[-1,-2],\ [p,p],\ [p+8,1]\rangle.
\end{aligned}$$

We can rewrite this group as $\mathrm{Sel}^{(2)}(\mathcal{E}_{-1},\mathbb{Q}) = \langle[-1,-2],[-p,-2p],[-p-8,-2]\rangle$, where $\mu(\mathcal{E}_{-1}(\mathbb{Q})[2]/2\mathcal{E}_{-1}(\mathbb{Q})) = \langle[-p,-2p],[-p-8,-2]\rangle$ and the rest of elements of the Selmer group come from points in $\mathcal{E}_{-1}(\mathbb{Q})$ that have infinite order.

So far, we have only used the first two conditions on p stated in the theorem 4.1; that p and $p+8$ and that $p \equiv p+8 \equiv 1 \pmod 8$. The third condition will give us that the rank of $\mathcal{E}(\mathbb{Q})$ is zero.

4.4 Quadratic reciprocity in $\mathbb{Q}(i)$

The notion of quadratic residue can be generalised to $\mathbb{Z}[i]$ in a natural way by setting[4] $\left[\frac{\mathfrak{a}}{\mathfrak{p}}\right] = 1$ for a prime $\mathfrak{p} \in \mathbb{Z}[i]$ and $\mathfrak{a} \in \mathbb{Z}[i] \setminus \mathfrak{p}$ if and only if there exists some $\mathfrak{b} \in \mathbb{Z}[i] \setminus \mathfrak{p}$ such that $\mathfrak{a} = \mathfrak{b}^2 \pmod{\mathfrak{p}}$.

To operate with residues in $\mathbb{Z}[i]$, there exist laws of quadratic reciprocity, which are closely linked to some of the laws of quartic reciprocity in $\mathbb{Z}$. A simplification of those laws is given by the following results:

Proposition 4.3. *Let $\mathfrak{p} = a+bi$, $\mathfrak{q} = c+di$ be two different primes in $\mathbb{Z}[i]$ such that $\mathfrak{p} \equiv \mathfrak{q} \equiv 1 \pmod 2$. Then,*

1. $\left[\frac{i}{\mathfrak{p}}\right] = (-1)^{b/2}$,
2. $\left[\frac{\mathfrak{p}}{\mathfrak{q}}\right] = \left(\frac{ac+bd}{\mathrm{N}_{\mathbb{Q}(i)/\mathbb{Q}}(\mathfrak{q})}\right)$,
3. $\left[\frac{\mathfrak{q}}{\mathfrak{p}}\right] = \left[\frac{\mathfrak{p}}{\mathfrak{q}}\right]$.

Proof. [Lem00, Proposition 5.1]. □

Proposition 4.4. *Let $p = a^2+b^2$ and $q = c^2+d^2$ be different primes such that $b \equiv d \equiv 0 \pmod 2$ and $\left(\frac{p}{q}\right) = 1$. Then,*

1. $\left(\frac{a}{p}\right) = 1$,
2. $\left(\frac{p}{q}\right)_4\left(\frac{q}{p}\right)_4 = \left(\frac{ac+bd}{p}\right)$. *(Burde's reciprocity law)*

Proof. [Lem00, Propositions 5.2 and 5.7]. □

Let us now analyse how p and $p+8$ behave in $\mathbb{Z}[i]$.

As $p \equiv 1 \pmod 8$, $p = a^2+b^2$ for some $a,b \in \mathbb{Z}$ and p splits into two primary primes $\mathfrak{p}_1 = a+bi$ and $\mathfrak{p}_2 = a-bi$ where b is even, such that $p = \mathfrak{p}_1\mathfrak{p}_2$. Similarly, as $p+8 \equiv 1 \pmod 8$, $p+8$ splits into two primes $\mathfrak{p}_3 = c+di$, $\mathfrak{p}_4 = c-di$ with d even. Therefore, $\mathfrak{p}_j \equiv 1 \pmod 2$.

[4] The notation is different to the one used for quadratic reciprocity in $\mathbb{Z}$ to distinguish when we are using one or another.

We then have the following results:

Proposition 4.5. *Let $p = a^2 + b^2$ and $p + 8 = c^2 + d^2$ be as in theorem 4.1 and $\mathfrak{p}_j \in \{1, 2, 3, 4\}$ as previously described. Then,*

1. $\mathfrak{p}_j \equiv 1$ *or* $3 \pmod{(1+i)^5}$, $\mathfrak{p}_1 \equiv \mathfrak{p}_2 \pmod{(1+i)^5}$ *and* $\mathfrak{p}_3 \equiv \mathfrak{p}_4 \pmod{(1+i)^5}$.
2. $\left[\frac{i}{\mathfrak{p}_j}\right] = 1$.
3. $\left[\frac{3}{\mathfrak{p}_1}\right] = \left[\frac{3}{\mathfrak{p}_2}\right] = -1$.
4. $\left[\frac{\mathfrak{p}_1}{\mathfrak{p}_2}\right] = \left[\frac{\mathfrak{p}_2}{\mathfrak{p}_1}\right] = \left[\frac{\mathfrak{p}_3}{\mathfrak{p}_4}\right] = \left[\frac{\mathfrak{p}_4}{\mathfrak{p}_3}\right] = 1$.
5. $\left[\frac{\mathfrak{p}_3}{\mathfrak{p}_1}\right] = \left[\frac{\mathfrak{p}_4}{\mathfrak{p}_1}\right] = \left[\frac{\mathfrak{p}_3}{\mathfrak{p}_2}\right] = \left[\frac{\mathfrak{p}_4}{\mathfrak{p}_2}\right] = -1$.
6. *There exists an* $n \in \mathbb{Z}$ *such that* $\left[\frac{n}{\mathfrak{p}_3}\right] = \left[\frac{n}{\mathfrak{p}_4}\right] = -1$ *and* $\left[\frac{n+8}{\mathfrak{p}_3}\right] = \left[\frac{n+8}{\mathfrak{p}_4}\right] = 1$.

Proof. 1. and 2. are a consequence of proposition 4.3 and the fact that $4|b$ and $4|d$.

3. $\mathrm{N}_{\mathbb{Q}(i)/\mathbb{Q}}(\mathfrak{p}_1) = \mathrm{N}_{\mathbb{Q}(i)/\mathbb{Q}}(\mathfrak{p}_2) = p$, so
$$\left[\frac{3}{\mathfrak{p}_1}\right] = \left[\frac{3}{\mathfrak{p}_2}\right] = \left(\frac{3a}{p}\right) = \left(\frac{3}{p}\right)\left(\frac{a}{p}\right) = -1.$$

4. From proposition 4.3 we get,
$$\left[\frac{\mathfrak{p}_1}{\mathfrak{p}_2}\right] = \left[\frac{\mathfrak{p}_2}{\mathfrak{p}_1}\right] = \left(\frac{a^2-b^2}{p}\right) = \left(\frac{2b^2}{p}\right) = 1, \qquad \left[\frac{\mathfrak{p}_3}{\mathfrak{p}_4}\right] = \left[\frac{\mathfrak{p}_4}{\mathfrak{p}_3}\right] = \left(\frac{c^2-d^2}{p+8}\right) = 1.$$

5. We will only prove one case, but a similar reasoning works for the rest.
$$\left[\frac{\mathfrak{p}_3}{\mathfrak{p}_1}\right] \overset{4.3}{=} \left(\frac{ac+bd}{p}\right) \overset{4.4}{=} \left(\frac{p}{p+8}\right)_4 \left(\frac{p+8}{p}\right)_4 = \left(\frac{-8}{p+8}\right)_4 \left(\frac{8}{p}\right)_4 = \left(\frac{2}{p+8}\right)_4 \left(\frac{2}{p}\right)_4 \overset{4.1}{=} -1$$
where the second-to-last equality is because
$$\left(\frac{-4}{p+8}\right)_4 = 1, \quad \text{as } \left(\frac{2}{p+8}\right) = 1 \text{ and } \left(\frac{-1}{p+8}\right)_4 = 1 \ (\text{as } p+8 \equiv 1 \pmod 8).$$
$$\left(\frac{4}{p}\right)_4 = 1, \quad \text{as } \left(\frac{2}{p}\right) = 1.$$

6. To prove this, it is key to realise that every element $x + yi \in \mathbb{Z}[i]$ is equivalent to an element in $\mathbb{Z}$ modulo $\mathfrak{p}_3$. This is because as c and d are coprime, by Bezout's theorem we can find elements $s, t \in \mathbb{Z}$ such that $sc + dt = y$ and so, $x + yi - (c + di)(t + si) \in \mathbb{Z}$. As $[n, \mathfrak{p}_3] = [n, \mathfrak{p}_4] = 1$ for every $n \in [-4, 4]$, by repeating the proof of proposition 4.1 we conclude. □

4.5 The 2-Selmer group of $\mathcal{E}$ over $\mathbb{Q}(i)$

The discriminant of $\mathcal{E}/\mathbb{Q}(i)$ is $\Delta = -(1+i)^{20}\,\mathfrak{p}_1^2\,\mathfrak{p}_2^2\,\mathfrak{p}_3^2\,\mathfrak{p}_4^2$, so the equation 4.1 might not be minimal at $\mathfrak{p} = 1+i$ as $v_{1+i}(\Delta) = 20 > 12$.

However, it is easy to see [Con99, Proposition 4.1.1] that every change of variables to get a minimal Weierstrass curve must be of the form

$$x = u^2x' + r \qquad\qquad y = u^3y' + u^2sx' + t$$

for some $u, r, s, t \in K$, $u \neq 0$.

Therefore, if $\mathcal{E}'$ is a minimal elliptic curve, $\Delta' = u^{-12}\Delta$ and as $12 \nmid 20$, we deduce that $(1+i)|\Delta'$ and, the set of all places where $\mathcal{E}'$ has bad reduction must be

$$\{1+i,\ \mathfrak{p}_1,\ \mathfrak{p}_2,\ \mathfrak{p}_3,\ \mathfrak{p}_4\}.$$

Thus,

$$S = \{\infty,\ 1+i,\ \mathfrak{p}_1,\ \mathfrak{p}_2,\ \mathfrak{p}_3,\ \mathfrak{p}_4\} \quad \text{and} \quad \mathbb{Q}(i)(S,2) = \langle i,\ 1+i,\ \mathfrak{p}_1,\ \mathfrak{p}_2,\ \mathfrak{p}_3,\ \mathfrak{p}_4\rangle,$$

so,

$$\begin{aligned}\mathbb{Q}(i)(S,2)\times\mathbb{Q}(i)(S,2) = \langle &[1,i],\ [1,1+i],\ [1,\mathfrak{p}_1],\ [1,\mathfrak{p}_2],\ [1,\mathfrak{p}_3],\ [1,\mathfrak{p}_4],\\ &[i,1],\ [1+i,1],\ [\mathfrak{p}_1,1],\ [\mathfrak{p}_2,1],\ [\mathfrak{p}_3,1],\ [\mathfrak{p}_4,1]\rangle.\end{aligned}$$

The map μ between $\mathcal{E}(\mathbb{Q}(i))/2\mathcal{E}(\mathbb{Q}(i))$ and $\mathbb{Q}(i)(S,2)\times\mathbb{Q}(i)(S,2)$ is as follows:

$$P = (x_P, y_P) \longmapsto \mu(P) = \begin{cases}[1,1] & \text{if } P = \underline{o}\\ [\mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_4, \mathfrak{p}_1\mathfrak{p}_2] & \text{if } x_P = 0\\ [\mathfrak{p}_1\mathfrak{p}_2, i\,\mathfrak{p}_1\mathfrak{p}_2] & \text{if } x_P = p\\ [x_P, x_P - p] & \text{if } x_P \neq 0,\ p\end{cases}$$

and $(p+8, 0) \overset{\mu}{\mapsto} [\mathfrak{p}_3\mathfrak{p}_4, i]$. Therefore,

$$\mu(\mathcal{E}(\mathbb{Q}(i))[2]/2\mathcal{E}(\mathbb{Q}(i))) = \langle[\mathfrak{p}_1\mathfrak{p}_2, i\,\mathfrak{p}_1\mathfrak{p}_2], [\mathfrak{p}_3\mathfrak{p}_4, i]\rangle.$$

As explained in example 2.5, $\mathbb{Q}(i)_\infty = \mathbb{C}$. Since $\mathcal{E}(\mathbb{C})/2\mathcal{E}(\mathbb{C})$ is trivial, restricting to $\mathbb{C}$ does not provide any help in finding the elements of $\mathrm{Sel}^{(2)}(\mathcal{E}/\mathbb{Q}(i))$, so it will suffice to analyse the restrictions to non-Archimedean places.

4.5.1 Restriction to $\mathbb{Q}(i)_{1+i}$

We start by considering $M_0 = \mathbb{Q}(i)(S,2) \times \mathbb{Q}(i)(S,2)$. We then have:

$$\begin{array}{ccc} \mathcal{E}(\mathbb{Q}(i))/2\mathcal{E}(\mathbb{Q}(i)) & \xrightarrow{\mu} & M_0 \\ \downarrow{\scriptstyle id_{1+i}} & & \downarrow{\scriptstyle j_{1+i}} \\ \mathcal{E}(\mathbb{Q}(i)_{1+i})/2\mathcal{E}(\mathbb{Q}(i)_{1+i}) & \xrightarrow{\mu_{1+i}} & (M_0)_{\mathbb{Q}(i)_{1+i}} \end{array}$$

From proposition 2.4, we know that $\mathbb{Q}(i)^\times_{1+i}/(\mathbb{Q}(i)^\times_{1+i})^2 = \langle i, 1+2i, 2+i, 1+i\rangle$ and proposition 3.4 gives us $\#\mathcal{E}(\mathbb{Q}(i)_{1+i})/2\mathcal{E}(\mathbb{Q}(i)_{1+i}) = 16$. As none of the $\mathfrak{p}_i$ is a multiple of $1+i$, their representatives in $\mathbb{Q}(i)^\times_{1+i}/(\mathbb{Q}(i)^\times_{1+i})^2$ will correspond to the remainder of dividing $\mathfrak{p}_i$ by $(1+i)^5$ which, by proposition 4.5, is either 1 or 3. Then,

$$(0,0) \xmapsto{\mu_{1+i}} [1,1], \qquad (p,0) \xmapsto{\mu_{1+i}} [1,i], \qquad (p-8,0) \xmapsto{\mu_{1+i}} [1,i].$$

Therefore, $(p,0)$ is a generator of $\mathcal{E}(\mathbb{Q}(i)_{1+i})/2\mathcal{E}(\mathbb{Q}(i)_{1+i})$. It is easy to check that the other three are given by

$$(p+12,\gamma_1), \qquad (p-4,\gamma_2), \qquad (p+4+8i,\gamma_3),$$

where the γ_i are such that the points are defined in $\mathcal{E}(\mathbb{Q}(i)_{1+i})$. Then,

$$\begin{aligned} (p+12,\gamma_1) &\xmapsto{\mu_{1+i}} [3,3], \\ (p-4,\gamma_2) &\xmapsto{\mu_{1+i}} [3,1+2i], \\ (p+4+8i,\gamma_3) &\xmapsto{\mu_{1+i}} [3,1], \end{aligned}$$

where $3 = i(1+2i)(2+i)$ in $\mathbb{Q}(i)^\times_{1+i}/(\mathbb{Q}(i)^\times_{1+i})^2$. Hence,

$$\begin{aligned} \mathcal{E}(\mathbb{Q}(i)_{i+1})/2\mathcal{E}(\mathbb{Q}(i)_{1+i}) &= \langle (p,0),\ (p+12,\gamma_1),\ (p-4,\gamma_2),\ (p+4+8i,\gamma_3)\rangle, \\ \operatorname{im}\mu_{1+i} &= \langle [1,i], [3,3],\ [3,1+2i],\ [3,1]\rangle. \end{aligned}$$

The images of the generators of M_0 under the map j_{1+i} are as follows:

$$\begin{array}{cccccc} [1,i] & [1,1+i] & [1,\mathfrak{p}_1] & [1,\mathfrak{p}_2] & [1,\mathfrak{p}_3] & [1,\mathfrak{p}_4] \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ [1,i] & [1,1+i] & [1,1 \text{ or } 3] & [1,1 \text{ or } 3] & [1,1 \text{ or } 3] & [1,1 \text{ or } 3] \\ [i,1] & [1+i,1] & [\mathfrak{p}_1,1] & [\mathfrak{p}_2,1] & [\mathfrak{p}_3,1] & [\mathfrak{p}_4,1] \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ [i,1] & [1+i,1] & [1 \text{ or } 3,1] & [1 \text{ or } 3,1] & [1 \text{ or } 3,1] & [1 \text{ or } 3,1] \end{array}$$

It is easy to see that $[1,1+i]$, $[i+1,1]$ and $[i,1]$ do not go to elements in $\operatorname{im}\mu_{1+i}$. As the rest of elements go to $\operatorname{im}\mu_{1+i}$, we deduce that

$$\begin{aligned} M_1 := M_0 \cap j_{1+i}^{-1}(\operatorname{im}\mu_{1+i}) = \langle &[1,i],\ [1,\mathfrak{p}_1],\ [1,\mathfrak{p}_2],\ [1,\mathfrak{p}_3],\ [1,\mathfrak{p}_4], \\ &[\mathfrak{p}_1,1],\ [\mathfrak{p}_2,1],\ [\mathfrak{p}_3,1],\ [\mathfrak{p}_4,1]\rangle. \end{aligned}$$

4.5.2 Restrictions to $\mathfrak{p}_1$ and $\mathfrak{p}_2$

By considering $M_2 \coloneqq M_1 \cap j_{\mathfrak{p}_1}(\operatorname{im}\mu_{\mathfrak{p}_1})$, we get the diagrams:

$$\begin{array}{ccc} \mathcal{E}(\mathbb{Q}(i))/2\mathcal{E}(\mathbb{Q}(i)) & \xrightarrow{\mu} & M_1 \\ \downarrow{\scriptstyle i_{\mathfrak{p}_1}} & & \downarrow{\scriptstyle j_{\mathfrak{p}_1}} \\ \mathcal{E}(\mathbb{Q}(i)_{\mathfrak{p}_1})/2\mathcal{E}(\mathbb{Q}(i)_{\mathfrak{p}_1}) & \xrightarrow{\mu_{\mathfrak{p}_1}} & (M_1)_{\mathfrak{p}_1} \end{array} \qquad \begin{array}{ccc} \mathcal{E}(\mathbb{Q}(i))/2\mathcal{E}(\mathbb{Q}(i)) & \xrightarrow{\mu} & M_2 \\ \downarrow{\scriptstyle i_{\mathfrak{p}_2}} & & \downarrow{\scriptstyle j_{\mathfrak{p}_2}} \\ \mathcal{E}(\mathbb{Q}(i)_{\mathfrak{p}_2})/2\mathcal{E}(\mathbb{Q}(i)_{\mathfrak{p}_2}) & \xrightarrow{\mu_{\mathfrak{p}_2}} & (M_2)_{\mathfrak{p}_2} \end{array}$$

From proposition 2.4, we know that $\mathbb{Q}_{\mathfrak{p}_1}^\times/(\mathbb{Q}_{\mathfrak{p}_1}^\times)^2 = \langle 3, \mathfrak{p}_1\rangle$ as $[\frac{3}{\mathfrak{p}_1}] = -1$, and also that $\#\mathcal{E}(\mathbb{Q}_{\mathfrak{p}_1})/2\mathcal{E}(\mathbb{Q}_{\mathfrak{p}_1}) = 4$. As

$$(0,0) \overset{\mu_p}{\longmapsto} [\mathfrak{p}_1, \mathfrak{p}_1], \qquad (-p,0) \overset{\mu_p}{\longmapsto} [\mathfrak{p}_1, \mathfrak{p}_1], \qquad (-p-8,0) \overset{\mu_p}{\longmapsto} [1,1],$$

we know that $(0,0)$ is one of the generators of $\mathcal{E}(\mathbb{Q}_{\mathfrak{p}_1})/2\mathcal{E}(\mathbb{Q}_{\mathfrak{p}_1})$. For the other generator, we can consider the point that we used before, $(p+6, \alpha)$, where α is the square root of $(p+6)\,6\,(-2)$ in $\mathbb{Q}_{\mathfrak{p}_1}^\times/(\mathbb{Q}_{\mathfrak{p}_1}^\times)^2$. Then, as $[\frac{6}{\mathfrak{p}_1}] = -1$, we get that $(p+6,\alpha) \overset{\mu_p}{\longmapsto} [3,3]$ and

$$\mathcal{E}(\mathbb{Q}_{\mathfrak{p}_1})/2\mathcal{E}(\mathbb{Q}_{\mathfrak{p}_1}) = \langle (0,0), (p+6,\alpha)\rangle, \qquad \operatorname{im}\mu_{\mathfrak{p}_1} = \langle [\mathfrak{p}_1,\mathfrak{p}_1], [3,3]\rangle.$$

As $\left[\frac{i}{\mathfrak{p}_1}\right] = \left[\frac{\mathfrak{p}_2}{\mathfrak{p}_1}\right] = 1$ and $\left[\frac{\mathfrak{p}_3}{\mathfrak{p}_1}\right] = \left[\frac{\mathfrak{p}_4}{\mathfrak{p}_1}\right] = -1$, the generators of M_1 under $j_{\mathfrak{p}_1}$ become:

$$\begin{array}{ccccccccc} [1,i] & [1,\mathfrak{p}_1] & [1,\mathfrak{p}_2] & [1,\mathfrak{p}_3] & [1,\mathfrak{p}_4] & [\mathfrak{p}_1,1] & [\mathfrak{p}_2,1] & [\mathfrak{p}_3,1] & [\mathfrak{p}_4,1] \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ [1,1] & [1,\mathfrak{p}_1] & [1,1] & [1,3] & [1,3] & [\mathfrak{p}_1,1] & [1,1] & [3,1] & [3,1] \end{array}$$

By multiplying the generators to each other, we can rearrange them to get that

$$M_1 = \langle [1,i],\ [1,\mathfrak{p}_2],\ [\mathfrak{p}_2,1],\ [1,\mathfrak{p}_1],\ [\mathfrak{p}_1,\mathfrak{p}_1],\ [1,\mathfrak{p}_3],\ [\mathfrak{p}_3,\mathfrak{p}_3],\ [\mathfrak{p}_3,\mathfrak{p}_4],\ [\mathfrak{p}_4,\mathfrak{p}_4]\rangle,$$

where all elements are sent to $\operatorname{im}\mu_{\mathfrak{p}_1}$ except for $[1,\mathfrak{p}_1]$ and $[1,\mathfrak{p}_3]$. Hence,

$$M_2 \coloneqq M_1 \cap j_{\mathfrak{p}_1}^{-1}(\operatorname{im}\mu_{\mathfrak{p}_1}) = \langle [1,i],\ [1,\mathfrak{p}_2],\ [\mathfrak{p}_2,1],\ [\mathfrak{p}_1,\mathfrak{p}_1],\ [\mathfrak{p}_3,\mathfrak{p}_3],\ [\mathfrak{p}_3,\mathfrak{p}_4],\ [\mathfrak{p}_4,\mathfrak{p}_4]\rangle.$$

For $\mathfrak{p}_2$, $\mathbb{Q}_{\mathfrak{p}_2}^\times/(\mathbb{Q}_{\mathfrak{p}_2}^\times)^2 = \langle 3, \mathfrak{p}_2\rangle$ and we can choose the same points as for $\mathfrak{p}_1$ to deduce that

$$\mathcal{E}(\mathbb{Q}_{\mathfrak{p}_2})/2\mathcal{E}(\mathbb{Q}_{\mathfrak{p}_2}) = \langle (0,0), (p+6,\alpha)\rangle, \qquad \operatorname{im}\mu_{\mathfrak{p}_2} = \langle [\mathfrak{p}_2,\mathfrak{p}_2], [3,3]\rangle.$$

As the images of the generators of M_2 under $j_{\mathfrak{p}_2}$ are

$$\begin{array}{ccccccc} [1,i] & [1,\mathfrak{p}_2] & [\mathfrak{p}_2,1] & [\mathfrak{p}_1,\mathfrak{p}_1] & [\mathfrak{p}_3,\mathfrak{p}_3] & [\mathfrak{p}_3,\mathfrak{p}_4] & [\mathfrak{p}_4,\mathfrak{p}_4] \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ [1,1] & [1,\mathfrak{p}_2] & [\mathfrak{p}_2,1] & [1,1] & [3,3] & [3,3] & [3,3] \end{array}$$

we deduce that

$$M_3 \coloneqq M_2 \cap j_{\mathfrak{p}_2}^{-1}(\operatorname{im}\mu_{\mathfrak{p}_2}) = \langle [1,i],\ [\mathfrak{p}_1,\mathfrak{p}_1],\ [\mathfrak{p}_2,\mathfrak{p}_2],\ [\mathfrak{p}_3,\mathfrak{p}_3],\ [\mathfrak{p}_3,\mathfrak{p}_4],\ [\mathfrak{p}_4,\mathfrak{p}_4]\rangle.$$

4.5.3 Restrictions to $\mathfrak{p}_3$ and $\mathfrak{p}_4$

By considering $M_4 := M_3 \cap j_{\mathfrak{p}_3}(\operatorname{im}\mu_{\mathfrak{p}_3})$, we get the diagrams:

$$\begin{array}{ccc} \mathcal{E}(\mathbb{Q}(i))/2\mathcal{E}(\mathbb{Q}(i)) & \xrightarrow{\mu} & M_3 \\ \downarrow{\scriptstyle i_{\mathfrak{p}_3}} & & \downarrow{\scriptstyle j_{\mathfrak{p}_3}} \\ \mathcal{E}(\mathbb{Q}(i)_{\mathfrak{p}_3})/2\mathcal{E}(\mathbb{Q}(i)_{\mathfrak{p}_3}) & \xrightarrow{\mu_{\mathfrak{p}_3}} & (M_3)_{\mathfrak{p}_3} \end{array} \qquad \begin{array}{ccc} \mathcal{E}(\mathbb{Q}(i))/2\mathcal{E}(\mathbb{Q}(i)) & \xrightarrow{\mu} & M_4 \\ \downarrow{\scriptstyle i_{\mathfrak{p}_4}} & & \downarrow{\scriptstyle j_{\mathfrak{p}_4}} \\ \mathcal{E}(\mathbb{Q}(i)_{\mathfrak{p}_4})/2\mathcal{E}(\mathbb{Q}(i)_{\mathfrak{p}_4}) & \xrightarrow{\mu_{\mathfrak{p}_4}} & (M_4)_{\mathfrak{p}_4} \end{array}$$

From proposition 4.5, we know that $\mathbb{Q}_{\mathfrak{p}_3}^{\times}/(\mathbb{Q}_{\mathfrak{p}_3}^{\times})^2 = \langle n, \mathfrak{p}_1\rangle$ where $[\frac{n}{p+8}] = -1$ and $[\frac{n+8}{p+8}] = 1$. We also know that $\#\mathcal{E}(\mathbb{Q}_{\mathfrak{p}_1})/2\mathcal{E}(\mathbb{Q}_{\mathfrak{p}_1}) = 4$ and

$$(0,0) \overset{\mu_{\mathfrak{p}_3}}{\longmapsto} [\mathfrak{p}_3, 1], \qquad (p,0) \overset{\mu_{\mathfrak{p}_3}}{\longmapsto} [1,1], \qquad (p+8,0) \overset{\mu_{\mathfrak{p}_3}}{\longmapsto} [\mathfrak{p}_3, 1],$$

so $(0,0)$ is a generator of $\mathcal{E}(\mathbb{Q}(i)_{\mathfrak{p}_3})/2\mathcal{E}(\mathbb{Q}(i)_{\mathfrak{p}_3})$. The other generator is given, as before, $(p+8+n, \beta_n)$, which satisfies that $(p+8+n, \beta_n) \overset{\mu_{\mathfrak{p}_3}}{\longmapsto} [n,1]$, so

$$\mathcal{E}(\mathbb{Q}_{\mathfrak{p}_3})/2\mathcal{E}(\mathbb{Q}_{\mathfrak{p}_3}) = \langle (0,0), (p+8+n, \beta_n)\rangle, \qquad \operatorname{im}\mu_{\mathfrak{p}_3} = \langle [\mathfrak{p}_3, 1], [n,1]\rangle.$$

The images of the generators of M_3 are

$$\begin{array}{cccccc} [1,i] & [\mathfrak{p}_1,\mathfrak{p}_1] & [\mathfrak{p}_2,\mathfrak{p}_2] & [\mathfrak{p}_3,\mathfrak{p}_3] & [\mathfrak{p}_3,\mathfrak{p}_4] & [\mathfrak{p}_4,\mathfrak{p}_4] \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ [1,1] & [n,n] & [n,n] & [\mathfrak{p}_3,\mathfrak{p}_3] & [\mathfrak{p}_3,1] & [1,1] \end{array}$$

Therefore, we deduce that

$$M_4 := M_3 \cap j_{\mathfrak{p}_3}(\operatorname{im}\mu_{\mathfrak{p}_3}) = \langle [1,i],\ [\mathfrak{p}_1\mathfrak{p}_2, \mathfrak{p}_1\mathfrak{p}_2],\ [\mathfrak{p}_3,\mathfrak{p}_4],\ [\mathfrak{p}_4,\mathfrak{p}_4]\rangle.$$

Finally, for $\mathfrak{p}_4$, $\mathbb{Q}_{\mathfrak{p}_4}^{\times}/(\mathbb{Q}_{\mathfrak{p}_4}^{\times})^2 = \langle n, \mathfrak{p}_4\rangle$ and we can choose the same points as for $\mathfrak{p}_3$ to deduce that

$$\mathcal{E}(\mathbb{Q}_{\mathfrak{p}_4})/2\mathcal{E}(\mathbb{Q}_{\mathfrak{p}_4}) = \langle (0,0), (p+8+n, \beta_n)\rangle, \qquad \operatorname{im}\mu_{\mathfrak{p}_4} = \langle [\mathfrak{p}_4, 1], [n,1]\rangle$$

and

$$\begin{array}{cccc} [1,i] & [\mathfrak{p}_1\mathfrak{p}_2,\mathfrak{p}_1\mathfrak{p}_2] & [\mathfrak{p}_3,\mathfrak{p}_4] & [\mathfrak{p}_4,\mathfrak{p}_4] \\ \downarrow & \downarrow & \downarrow & \downarrow \\ [1,1] & [1,1] & [1,\mathfrak{p}_4] & [\mathfrak{p}_4,\mathfrak{p}_4] \end{array}$$

implying

$$\mathrm{Sel}^{(2)}(\mathcal{E}/\mathbb{Q}(i)) = \langle [1,i],\ [\mathfrak{p}_1\mathfrak{p}_2, \mathfrak{p}_1\mathfrak{p}_2],\ [\mathfrak{p}_3\mathfrak{p}_4, 1]\rangle.$$

We can then rewrite this group as $\mathrm{Sel}^{(2)}(\mathcal{E}/\mathbb{Q}(i)) = \langle [1,i],\ [\mathfrak{p}_1\mathfrak{p}_2, i\mathfrak{p}_1\mathfrak{p}_2],\ [\mathfrak{p}_3\mathfrak{p}_4, i]\rangle$, where $\mu(\mathcal{E}(\mathbb{Q}(i))[2]/2\mathcal{E}(\mathbb{Q}(i))) = \langle [\mathfrak{p}_1\mathfrak{p}_2, i\mathfrak{p}_1\mathfrak{p}_2],\ [\mathfrak{p}_3\mathfrak{p}_4, i]\rangle$.

This computation finishes the proof of theorem 4.1. □

4.6 Generalisations of the counterexample

It might not be immediately evident why the conditions of theorem 4.1 are all necessary. However, by breaking down all the conditions, one can see why they are indeed necessary to obtain curves with non-trivial $Ш(\mathcal{E}/\mathbb{Q})[2]$. First, we are going to see what happens when we do not impose that $p \equiv p+8 \equiv 1 \pmod 8$.

Proposition 4.6. *Let $p \in \mathbb{Z}$ such that p and $p+8$ are both primes and let*

$$\mathcal{E}\colon y^2 = x(x-p)(x-p-8).$$

Then,

- *If $p \equiv -3 \pmod 8$, $\operatorname{rank}_{\mathbb{Z}}(\mathcal{E}(\mathbb{Q})) = 1$.*
- *If $p \equiv -1 \pmod 8$, $\operatorname{rank}_{\mathbb{Z}}(\mathcal{E}(\mathbb{Q})) = 0$.*
- *If $p \equiv \ \ 3 \pmod 8$, $\operatorname{rank}_{\mathbb{Z}}(\mathcal{E}(\mathbb{Q})) = 0$.*

In all of these cases, $Ш(\mathcal{E}/\mathbb{Q})[2]$ is trivial. [5]

Proof. By repeating the same procedure used in section 4.2, we get that if $p \equiv -3 \pmod 8$, then

$$\mathrm{Sel}^{(2)}(\mathcal{E}/\mathbb{Q}) = \langle [1,-1],\ [p+8,2],\ [p,2p] \rangle,$$

and if $p \equiv -1, 3 \pmod 8$,

$$\mathrm{Sel}^{(2)}(\mathcal{E}/\mathbb{Q}) = \langle [p+8,2],\ [p,2p] \rangle.$$

The differences to the last proof are mostly due to the fact that in these cases -1 and 2 may not be quadratic residues modulo p, which affects $\operatorname{im} j_2$, $\operatorname{im} j_p$ and $\operatorname{im} j_{p+8}$. □

If we assume that $p \equiv p+8 \equiv 1$, but now allow

$$\left(\frac{2}{p}\right)_4 = \left(\frac{2}{p+8}\right)_4 = 1 \qquad \text{or} \qquad \left(\frac{2}{p}\right)_4 = \left(\frac{2}{p+8}\right)_4 = -1,$$

we have the following result:

Proposition 4.7. *Let $p \equiv p+8 \equiv 1 \pmod 8$ such that $\left(\frac{2}{p}\right)_4 = \left(\frac{2}{p+8}\right)_4$ and let*

$$\mathcal{E}\colon y^2 = x(x-p)(x-p-8).$$

Then,

$$\mathrm{Sel}^{(2)}(\mathcal{E}/\mathbb{Q}(i)) = \langle [1,i],\ [\mathfrak{p}_1,\mathfrak{p}_1],\ [\mathfrak{p}_2,\mathfrak{p}_2],\ [\mathfrak{p}_3,1],\ [\mathfrak{p}_4,1] \rangle.$$

Proof. If $\left(\frac{2}{p}\right)_4 = \left(\frac{2}{p+8}\right)_4$, the proposition 4.5 shows that $\left[\frac{\mathfrak{p}_i}{\mathfrak{p}_j}\right] = 1$ for every choice of $\mathfrak{p}_i, \mathfrak{p}_j$ and repeating the process from section 4.4 gives us the desired result. □

[5] For the case where $p \equiv -3 \pmod 8$, we would still need to assume that $Ш(\mathcal{E}/\mathbb{Q})$ is finite

In this case, as $\operatorname{rank}_{\mathbb{Z}/2\mathbb{Z}} \mathrm{Sel}^{(2)}(\mathcal{E}/\mathbb{Q}(i)) = 5$, it gives us the rank bound

$$1 \leq \operatorname{rank}_{\mathbb{Z}} \mathcal{E}(\mathbb{Q}(i)) \leq 3,$$

and we cannot conclude that $\operatorname{rank}_{\mathbb{Z}} \mathcal{E}(\mathbb{Q}) = 0$ anymore.

Interestingly enough, by studying the rank of the curves with MAGMA [BCP979] (appendix B), there are some values of p for which $\operatorname{rank}_{\mathbb{Z}} \mathcal{E}(\mathbb{Q}) = 2$, while for others $\operatorname{rank}_{\mathbb{Z}} \mathcal{E}(\mathbb{Q}) = 0$ (table A.3).

In the first case, we deduce that $Ш(\mathcal{E}/\mathbb{Q})[2]$ is trivial, whereas in the last case, not only can we deduce that $Ш(\mathcal{E}/\mathbb{Q})[2] = (\mathbb{Z}/2\mathbb{Z})^2$, but also that $\operatorname{rank}_{\mathbb{Z}} \mathcal{E}(\mathbb{Q}(i)) = 1$, so $Ш(\mathcal{E}/\mathbb{Q}(i))[2] = (\mathbb{Z}/2\mathbb{Z})^2$. Therefore, the homogeneous spaces associated to the elements of $\mathrm{Sel}^{(2)}(\mathcal{E}/\mathbb{Q}(i))$ that do not correspond to points in $\mathcal{E}(\mathbb{Q}(i))$ would satisfy an even more general instance of the Hasse principle, in which the equation also has solutions in $\mathbb{Q}(i)_{\mathfrak{p}}$ for every place $\mathfrak{p}$ of $\mathbb{Q}(i)$, but has no solutions in $\mathbb{Q}(i)$.

4.7 Conclusion

Other methods that have not been discussed in this dissertation have also been used to analyse the equation 4.1, such as **descent by 2-isogeny** [Sil09, Proposition 4.9], **second descent** [Con99, Section 3.6.6] and **general 2-descent** [PSZ03, Section 7.6].

Nevertheless, the method of section 3.5 has proven to be the **most effective** one, as not having to explicitly solve the equations of the homogeneous spaces allows us to compute the 2-Selmer group in a succinct manner. Moreover, we have been able to gain information about the properties that p must satisfy for $\operatorname{rank}_{\mathbb{Z}/2\mathbb{Z}} Ш(\mathcal{E}/K)[2] > 0$, in a way that can be applied to analyse other families of elliptic curves depending on prime parameters. These analysis will shed light on the properties of the elliptic curves with non-trivial Tate-Shaferevich group, contributing to our understanding of this puzzling, yet exciting group.

Appendices

A | Tables

A.1 Some primes satisfying proposition 2.6

q_1	q_2	q_1	q_2	q_1	q_2	q_1	q_2	q_1	q_2	q_1	q_2
17	2	97	43	137	109	233	71	241	191	257	227
17	13	97	47	193	2	233	89	241	193	257	239
41	2	97	53	193	3	233	101	241	211	257	241
41	5	97	61	193	7	233	107	241	223	281	2
41	23	97	73	193	23	233	109	241	229	281	5
41	31	97	79	193	31	233	113	241	233	281	7
41	37	97	89	193	43	233	131	241	239	281	17
73	2	113	2	193	59	233	157	257	2	281	29
73	3	113	7	193	67	233	167	257	11	281	31
73	19	113	11	193	83	233	173	257	13	281	43
73	23	113	13	193	97	233	181	257	17	281	53
73	37	113	31	193	101	233	197	257	23	281	59
73	41	113	41	193	107	233	229	257	29	281	79
73	61	113	53	193	109	241	2	257	31	281	101
73	67	113	61	193	131	241	3	257	59	281	109
73	71	113	83	193	137	241	5	257	61	281	137
89	2	113	97	193	139	241	29	257	67	281	149
89	5	113	109	193	151	241	41	257	73	281	157
89	11	137	2	193	157	241	47	257	79	281	163
89	17	137	7	193	179	241	53	257	89	281	167
89	47	137	11	193	181	241	59	257	113	281	181
89	53	137	17	193	191	241	61	257	137	281	191
89	67	137	19	233	2	241	67	257	139	281	211
89	71	137	37	233	7	241	79	257	157	281	223
89	73	137	59	233	13	241	83	257	173	281	241
89	79	137	61	233	19	241	97	257	193	281	263
97	2	137	73	233	23	241	107	257	197	281	271
97	3	137	101	233	29	241	113	257	199	281	277
97	11	137	103	233	31	241	151	257	211		
97	31	137	107	233	37	241	181	257	223		

A.2 Some primes satisfying theorem 4.1

p	$\left(\frac{2}{p}\right)_4$	$\left(\frac{2}{p+8}\right)_4$	p	$\left(\frac{2}{p}\right)_4$	$\left(\frac{2}{p+8}\right)_4$	p	$\left(\frac{2}{p}\right)_4$	$\left(\frac{2}{p+8}\right)_4$	p	$\left(\frac{2}{p}\right)_4$	$\left(\frac{2}{p+8}\right)_4$
89	1	−1	22433	−1	1	42929	−1	1	69473	−1	1
233	1	−1	22769	−1	1	43313	1	−1	70241	−1	1
569	−1	1	23201	−1	1	43793	1	−1	70313	−1	1
929	−1	1	23753	−1	1	43961	−1	1	70841	1	−1
1289	1	−1	23993	1	−1	44249	−1	1	71081	−1	1
1481	1	−1	24113	−1	1	44273	1	−1	73361	1	−1
2081	−1	1	24329	1	−1	44633	1	−1	77681	−1	1
2129	1	−1	24473	1	−1	45329	1	−1	78233	1	−1
3041	−1	1	25793	1	−1	47129	1	−1	78569	1	−1
3209	−1	1	25841	−1	1	47513	1	−1	78713	−1	1
3449	1	−1	26489	−1	1	48809	−1	1	79193	1	−1
3761	1	−1	26633	1	−1	50849	−1	1	79769	1	−1
4649	−1	1	27329	1	−1	50993	1	−1	81401	−1	1
4721	1	−1	27809	1	−1	52313	−1	1	81761	−1	1
4793	−1	1	28289	−1	1	52553	1	−1	81929	−1	1
6113	−1	1	28649	−1	1	53609	−1	1	82721	1	−1
6473	−1	1	29009	−1	1	53849	1	−1	84449	1	−1
6569	1	−1	29129	−1	1	55001	1	−1	86201	1	−1
6833	−1	1	29753	−1	1	55049	1	−1	86249	−1	1
7529	1	−1	30089	1	−1	55889	1	−1	87041	−1	1
8081	1	−1	30161	1	−1	56921	−1	1	87641	1	−1
8369	1	−1	30809	−1	1	58313	1	−1	88793	1	−1
8753	−1	1	31649	1	−1	58913	−1	1	90281	1	−1
9689	−1	1	31721	1	−1	60209	−1	1	91961	−1	1
10169	−1	1	32369	−1	1	60449	1	−1	92033	−1	1
12401	−1	1	33521	1	−1	60953	1	−1	92369	−1	1
12689	−1	1	34361	1	−1	61121	−1	1	92849	−1	1
12713	1	−1	34721	1	−1	61553	1	−1	92993	1	−1
15233	−1	1	35393	−1	1	61673	1	−1	93329	1	−1
15809	1	−1	35969	−1	1	62129	1	−1	94049	1	−1
15881	1	−1	36209	1	−1	62753	−1	1	95561	1	−1
16361	1	−1	36713	−1	1	62921	−1	1	96329	−1	1
16553	1	−1	37361	1	−1	63353	1	−1	97073	−1	1
16649	1	−1	37529	−1	1	64601	1	−1	97553	1	−1
17033	1	−1	37889	−1	1	66161	1	−1	97841	1	−1
17489	−1	1	38321	1	−1	66449	−1	1	98009	1	−1
17921	−1	1	38729	1	−1	66593	1	−1	98729	1	−1
18041	1	−1	39233	1	−1	67121	−1	1	98801	−1	1
19793	1	−1	40841	1	−1	67481	−1	1	99713	−1	1
20849	−1	1	41513	−1	1	68729	1	−1	99809	−1	1
20921	1	−1	41729	1	−1	68993	−1	1			

A.3 Some primes for which $Ш(\mathcal{E}/\mathbb{Q}(i))[2] = (\mathbb{Z}/2\mathbb{Z})^2$

p	$\left(\frac{2}{p}\right)_4$	$\left(\frac{2}{p+8}\right)_4$	p	$\left(\frac{2}{p}\right)_4$	$\left(\frac{2}{p+8}\right)_4$	p	$\left(\frac{2}{p}\right)_4$	$\left(\frac{2}{p+8}\right)_4$
449	-1	-1	35801	1	1	70913	1	1
593	1	1	37049	1	1	71153	1	1
2273	1	1	37313	1	1	71249	1	1
5273	-1	-1	37649	-1	-1	72161	-1	-1
5849	-1	-1	38273	1	1	73553	1	1
6353	1	1	37649	-1	-1	73673	-1	-1
6521	1	1	39089	-1	-1	75161	-1	-1
7673	-1	-1	39761	1	1	75329	1	1
8009	-1	-1	39929	-1	-1	77369	-1	-1
8513	-1	-1	40169	1	1	77513	-1	-1
8681	-1	-1	41801	-1	-1	78041	1	1
9041	-1	-1	42641	-1	-1	79601	1	1
10313	-1	-1	42689	-1	-1	81041	1	1
11489	-1	-1	45833	-1	-1	83609	-1	-1
11681	-1	-1	47969	-1	-1	87473	-1	-1
12281	-1	-1	49169	-1	-1	88169	1	1
12569	1	1	49193	1	1	88721	1	1
13241	-1	-1	49409	1	1	89009	1	1
13913	1	1	49529	-1	-1	89513	-1	-1
17393	-1	-1	51473	-1	-1	89681	-1	-1
18089	-1	-1	52361	-1	-1	90473	-1	-1
19073	-1	-1	54401	1	1	91121	1	1
19433	1	1	54713	1	1	92753	1	1
21569	1	1	56393	-1	-1	93089	1	1
26729	-1	-1	57689	1	1	94841	1	1
27689	-1	-1	58049	1	1	95393	-1	-1
27953	1	1	59273	1	1	95873	-1	-1
29201	1	1	59369	-1	-1	96281	-1	-1
29633	-1	-1	59921	-1	-1	97169	1	1
29873	-1	-1	60161	-1	-1	98369	-1	-1
31481	-1	-1	65609	1	1	99233	-1	-1
33713	1	1	70289	1	1			

B | Code

In this section we will present the code programmed in MAGMA that has been used to analyse the elliptic curve 4.1. The code can be run in this online calculator (though calculations are restricted to 120 seconds).

B.1 Calculation of the primes in table A.2

```
Pr := PrimesInInterval(1, 100000); // Computes the list of all
    the primes smaller than 100000
lPr := #Pr; // Finds the length of Pr
TPr := [* *];
for n in [1 .. lPr] do
   if (Pr[n] mod 8) eq 1 then // Selects the primes 1 (mod 8)
      if IsPrime(Pr[n]+8) then // Selects the primes with p+8
          also prime
         // In this case 2 is a quartic residue modulo p if and
             only if p=a^2+b^2 with a*b=0 (mod 8)[6]
         _, x1, y1 := NormEquation(1, Pr[n]); // Computes the
             value of x1 and y1 such that p=x1^2+y1^2
         _, x2, y2 := NormEquation(1, Pr[n]+8); // Computes the
             value of x1 and y1 such that p=x2^2+y2^2
         if not (x1*y1 mod 8) eq (x2*y2 mod 8) then // Computes
             whether 2 is a quartic residue mod p and p+8 and
             chooses the appropriate p
            TPr := Append(TPr, Pr[n]); // Adds the elements to a
                list
         end if;
      end if;
   end if;
end for;
TPr;       // Returns the list
```

[6] [Sil09, Proposition X.6.6]

B.2 Main functions regarding elliptic curves

```
TPr;  // A list of numbers
lTPr=#TPr;
for n in [1 .. lTPr] do
   E := EllipticCurve([0,-2*TPr[n]-8,0,TPr[n]^2+8*TPr[n],0]); //
      Defines the elliptic curve of theorem 4.1 over the
      rationals (the 5 parameters correspond to the a_i of E in
      Weierstrass form)
   E1 := QuadraticTwist(E,-1); // Computes the quadratic twist of
       E with respect to -1
   PQ<x> := PolynomialRing(RationalField());
   Ki := NumberField(x^2+1); // Defines the number field Q(i)
   Ei := EllipticCurve([Ki|0,-2*TPr[n]-8,0,TPr[n]^2+8*TPr[n],0]);
       // Defines the elliptic curve over Q(i)
   IsMinimalModel(E); // Checks if the equation that defines E is
       minimal
   MinimalModel(E); // Returns a minimal equation of an elliptic
      curve (works as long as E is defined over Q or a number
      field of class 1).
   BadPrimes(E); // Returns the primes of bad reduction
   TorsionSubgroup(E); // Returns the torsion group of E
   TwoTorsionSubgroup(E); // Returns the 2-torsion group of E and
       it is faster than the previous function
   Rank(E); // Returns the exact rank of E or otherwise a lower
      bound for E
   RankBounds(E); // Returns an upper and a lower bound of the
      rank of E
   MordellWeilGroup(E); // Describes the Mordell-Weil group of E
   Generators(E); // Returns the generators of the Mordell-Weil
      group of E
   TwoSelmerGroup(E); // Returns the 2-Selmer group of E and the
      relations between their elements
   MordellWeilShaInformation(E:ShaInfo); // In addition to
      returning the information about the Mordell-Weil group, it
       returns bounds of the 2-torsion and 4-torsion part of the
       Tate-Shaferevich group
end for;
```

B.3 Calculation of the primes in table A.3

```
// The first part of the code is a repetition of section B.1, in
   order to obtain the primes of proposition 4.7

  Pr := PrimesInInterval(1, 100000);
  lPr := #Pr;
  TPr := [* *];
  for n in [1 .. lPr] do
     if (Pr[n] mod 8) eq 1 then
        if IsPrime(Pr[n]+8) then
           _, x1, y1 := NormEquation(1, Pr[n]);
           _, x2, y2 := NormEquation(1, Pr[n]+8);
           if (x1*y1 mod 8) eq (x2*y2 mod 8) then // Computes
              whether 2 is a quartic residue mod p and p+8 and
              chooses the appropriate p, which are the opposite as
               in section B.1
              TPr := Append(TPr, Pr[n]);
           end if;
        end if;
     end if;
  end for;
  lTPr := #TPr;
  SPr := [* *];
  for n in [1 .. lTPr] do
     E := EllipticCurve([0,-2*TPr[n]-8,0,TPr[n]^2+8*TPr[n],0]);
     Rnk := Rank(E); // Finds the rank of E
     if (Rnk eq 0) then
        SPr := Append(SPr, TPr[n]); // Select those with rank 0
     end if;
  end for;
  SPr; // Returns the list
```

Bibliography

[BCP979] Wieb Bosma, John Cannon, and Catherine Playoust, *The MAGMA Algebra System I: The User Language*, Journal of Symbolic Computation **24** (19979), no. 3-4, 235–265. ↑41

[Bro81] Ezra Brown, *The First Proof of the Quadratic Reciprocity Law, Revisited*, The American Mathematical Monthly **88** (1981), no. 4, 257. ↑12

[Cas62] John William Scott Cassels, *Arithmetic on Curves of Genus 1. IV. Proof of the Hauptvermutung.*, Journal für die reine und angewandte Mathematik (Crelles Journal) **1962** (1962), no. 211, 95–112. ↑23

[Cas67] John William Scott Cassels, *Survey Article-Diophantine Equations with Special Reference to Elliptic Curves*, Journal of the London Mathematical Society **s1-42** (1967), no. 1, 183–183. ↑13, 22

[Cas86] John William Scott Cassels, *Local Fields*, Vol. 2507, Cambridge University Press, 1986. ↑7, 9, 12

[Cas91] John William Scott Cassels, *LMSST: Lectures on Elliptic Curves*, Vol. 53, Cambridge University Press, Cambridge, 1991. ↑14

[CF96] John William Scott Cassels and E. Victor Flynn, *Prolegomena to a Middlebrow Arithmetic of Curves of Genus 2*, Cambridge University Press, 1996. ↑23, 24, 25

[Con99] Ian Connell, *Elliptic Curve Handbook*, Online notes, McGill University, 1999. https://webs.ucm.es/BUCM/mat/doc8354.pdf. ↑14, 15, 16, 36, 41

[Con] Keith Conrad, *Hensel's lemma*, Expository papers, University of Connecticut. https://kconrad.math.uconn.edu/blurbs/gradnumthy/hensel.pdf. ↑9

[Fly18] E. Victor Flynn, *Arbitrarily large Tate–Shafarevich group on Abelian surfaces*, Journal of Number Theory **186** (2018), 248–258. ↑23

[FR03] E. Victor Flynn and J. Redmond, *Application of covering techniques to families of curves*, Journal of Number Theory **101** (2003), no. 2, 376–397. ↑23

[Gou20] Fernando Q. Gouvêa, *p-adic Numbers*, Universitext, Springer International Publishing, Cham, 2020. ↑5, 7, 8

[Har20] David Harari, *Galois Cohomology and Class Field Theory*, Universitext, Springer International Publishing, Cham, 2020. ↑17, 19, 21

[Lem00] Franz Lemmermeyer, *Reciprocity Laws*, Springer Monographs in Mathematics, Springer Berlin Heidelberg, Berlin, Heidelberg, 2000. ↑34

[Lin40] Carl Erik Lind, *Untersuchungen über die rationalen Punkte der ebenen kubischen Kurven vom Geschlecht Ein*, Ph.D. Thesis, 1940. ↑13

[Mil86] James S. Milne, *Arithmetic Duality Theorems*, 1st ed., Academic Press, Inc., Boston, 1986. ↑24

[Neu99] Jürgen Neukirch, *Algebraic Number Theory*, Grundlehren der mathematischen Wissenschaften, vol. 322, Springer Berlin Heidelberg, Berlin, Heidelberg, 1999. ↑7, 8

[PSZ03] Attila Pethö, Susanne Schmitt, and Horst G. Zimmer, *Elliptic Curves*, de Gruyter Studies in Mathematics, Walter de Gruyter, Berlin, New York, 2003. ↑17, 23, 25, 41

[Rei42] Hans Reichardt, *Einige im Kleinen überall lösbare, im Großen unlösbare diophantische Gleichungen.*, Journal für die reine und angewandte Mathematik (Crelles Journal) **1942** (1942), no. 184, 12–18. ↑13

[Sel51] Ernst S. Selmer, *The Diophantine equation* $ax^3 + by^3 + cz^3 = 0$., Acta Mathematica **85** (1951), 203–362. ↑13

[Ser73] Jean-Pierre Serre, *A Course in Arithmetic*, Graduate Texts in Mathematics, vol. 7, Springer New York, New York, NY, 1973. ↑13

[Sil09] Joseph H. Silverman, *The Arithmetic of Elliptic Curves*, Graduate Texts in Mathematics, vol. 106, Springer New York, New York, NY, 2009. ↑15, 17, 18, 20, 21, 22, 41, 46

[Sut17] Andrew Sutherland, *Course 18.785 - Number Theory I*, Massachusetts Institute of Technology, MIT, Massachussets, 2017. https://math.mit.edu/classes/18.785/2017fa/. ↑6, 7

[Wei55] Andre Weil, *On Algebraic Groups and Homogeneous Spaces*, American Journal of Mathematics **77** (1955), no. 3, 493. ↑20