Applications of $S'$-unit Equations to the Arithmetic of Elliptic Curves

by

Angelos Koutsianas

Thesis
Submitted to the University of Warwick
for the degree of
Doctor of Philosophy

Mathematics Institute
September 2016
Στη σύζυγό μου Κέλλυ
και στον γιο μου Κωνσταντίνο
## Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Acknowledgements</td>
<td>iv</td>
</tr>
<tr>
<td>Declaration</td>
<td>vi</td>
</tr>
<tr>
<td>Abstract</td>
<td>vii</td>
</tr>
<tr>
<td>1 Introduction</td>
<td>1</td>
</tr>
<tr>
<td>2 Background</td>
<td>5</td>
</tr>
<tr>
<td>2.1 Elliptic curves</td>
<td>6</td>
</tr>
<tr>
<td>2.2 Number fields</td>
<td>16</td>
</tr>
<tr>
<td>2.2.1 S-properties</td>
<td>16</td>
</tr>
<tr>
<td>2.2.2 Hilbert symbol</td>
<td>18</td>
</tr>
<tr>
<td>2.2.3 More results</td>
<td>19</td>
</tr>
<tr>
<td>2.3 $p$–adic analysis</td>
<td>20</td>
</tr>
<tr>
<td>2.4 Kummer theory</td>
<td>21</td>
</tr>
<tr>
<td>2.5 Lattices</td>
<td>27</td>
</tr>
<tr>
<td>2.6 S–unit equation</td>
<td>29</td>
</tr>
<tr>
<td>2.7 Cremona–Lingham method</td>
<td>30</td>
</tr>
<tr>
<td>3 Using λ–invariant</td>
<td>33</td>
</tr>
<tr>
<td>4 Constructing 2–division fields</td>
<td>36</td>
</tr>
<tr>
<td>4.1 Quadratic extensions</td>
<td>36</td>
</tr>
<tr>
<td>4.2 Cubic extensions</td>
<td>37</td>
</tr>
<tr>
<td>4.2.1 The case $\zeta_3 \in K$</td>
<td>37</td>
</tr>
<tr>
<td>4.2.2 The case $\zeta_3 \notin K$</td>
<td>37</td>
</tr>
<tr>
<td>4.3 $S_3$ extensions</td>
<td>38</td>
</tr>
<tr>
<td>4.4 Example</td>
<td>41</td>
</tr>
<tr>
<td>4.5 Algorithms</td>
<td>44</td>
</tr>
</tbody>
</table>
# Solving $S$–unit equations

5.1 Algorithms for solving $S$–unit equations ........................................ 47
5.2 Reduce the number of $S$–unit equations ................................................ 48
5.3 Reducing the rank .................................................................................. 51
5.3.1 Gal($L/K$) is trivial ........................................................................... 52
5.3.2 Gal($L/K$) $\cong C_2$ ........................................................................ 52
5.3.3 Gal($L/K$) $\cong C_3$ ........................................................................ 53
5.3.4 Gal($L/K$) $\cong S_3$ ........................................................................ 54
5.4 Example .................................................................................................. 56

# Efficient Sieve

6.1 Trivial solutions for $|x - 1|_p \ll 1$ ......................................................... 63
6.1.1 Infinite place ..................................................................................... 64
6.1.2 Finite place ....................................................................................... 65
6.2 Decomposing the solutions ..................................................................... 68
6.2.1 Quadratic extensions ........................................................................ 69
6.2.2 Cubic extensions ............................................................................... 73
6.2.3 $S_3$ extensions ................................................................................ 74
6.3 Computing solutions ............................................................................. 77
6.3.1 Quadratic case .................................................................................. 78
6.3.2 Cubic case ....................................................................................... 79
6.3.3 $S_3$ case ......................................................................................... 82
6.3.4 Lifting congruence solutions ............................................................ 84
6.3.5 Final step .......................................................................................... 86
6.4 Identifying $S$–units efficiently ............................................................... 87
6.5 Example .................................................................................................. 88

# Conclusion

7. Conclusion ............................................................................................... 98

# Bibliography

Bibliography ............................................................................................... 100
I would first like to thank my supervisor, professor John Cremona. His constant encouragement and support was the most crucial factor for the completion of this thesis. His office was always open not only to talk about mathematics but also everyday life’s difficulties. His passion for number theory still makes me to try more and work harder and harder.

I would also want to thank all the staff of Warwick Mathematics Institute for the very friendly and cosy working environment. I am grateful to all the members of the number theory group I met during my studies, for the long discussions I had with all of them in the Common Room and during the group meetings.

My warm thanks to my friends Martha Giannoudovardi and Stephanos Papanikolopoulos for their warm welcome in UK, their hospitality and tasty food. Many thanks to my friends Alejandro Argaez, Italo Cipraja, Agelos Georgakopoulos, Panagiotis Gianniotis, Francesca Iezzi, Norihisa Ikoma, Aleks Jevnikar, Kuzma Khrabrov, Damiano Lupi, Gabriele Mancini, Theodoros Manikas, Marc Masdeu, Giannis Moutsinas, Sara Muhvic, Pantelis Samartsidis, Daniel Seco, Haluk Sengun, Jeroen Sijsling, Anna Tamarit, Damiano Testa, Simone Tiberi, Rosenberg Toala, Panayiota Touloupou and Konstantinos Tyros for making my stay in UK more comfortable and nicer. My special thanks to Samuele Anni for his cooking
skills and the fantastic Italian food.

My warm thanks to my friends Vasilis Noulopoulos, Dario Papavassiliou and Nikos Zygouras for the excellent nights we spent playing Greek folk music.

My thanks to my friends from Warwick Sport Centre with whom I used to play football every Tuesday and Friday evening.

I also want to thank miss Carole Fisher who never said no to any of the documents I asked her to write for me.

I am grateful to all my teachers of mathematics for what they have taught me.

I would like to thank my parents and my brother for their constant support during all these years.

Finally, I would like to thank the Academy of Athens and Bekiari–Vekri foundation for funding a part of my studies.
Declaration

I hereby declare that this thesis has been composed by myself and all the work in it is my own, unless otherwise stated. In Chapter 2 we present basic background material which can be found in the literature. Chapters 3, 4, 5 and 6 are my own work, unless otherwise indicated.
Abstract

Let $K$ be a number field and $S$ a finite set of prime ideals of $K$. By a classical result of Shafarevich ([Sil86]) we know that there are finitely many isomorphism classes $\mathcal{E}_{K,S}$ of elliptic curves defined over $K$ with good reduction outside $S$. Many people have developed methods of computing $\mathcal{E}_{K,S}$ explicitly. At the end, all the methods ask for solutions of specific Diophantine equations in order to determine $\mathcal{E}_{K,S}$. In this thesis we develop a new algorithmic method of computing $\mathcal{E}_{K,S}$ by solving $S$–unit equations.

The method is implemented in the mathematical software Sage ([Dev16]) and examples are included in this thesis.
Chapter 1

Introduction

The development of computers during the second half of 20th century has extremely affected modern science including modern mathematics. As a result computational mathematics has been a very rich, useful and necessary area of mathematics the last 60 years. Even in number theory and arithmetic geometry which were considered as the most ‘abstract’ areas of mathematics computations play an crucial role. For example, one of the 7 millennium problems in mathematics, the Birch and Swinnerton-Dyer conjecture (BSD), was a consequence of much experimental evidence ([BSD63], [BSD65]). Moreover, the huge LMFDB project ([LMF16]) is the biggest collection of data of the most important mathematical objects of modern number theory and arithmetic geometry.

One of the first and systematic collections of data in arithmetic geometry with the use of computers is Cremona’s tables ([Cre97]). Cremona uses the theory of modular symbols to compute all elliptic curves over $\mathbb{Q}$ of given conductor. One can try to do the same computations over a general number $K$ or ask the following more general question,
**Question 1.1.** Given a number field $K$ and a finite set $S$ of prime ideals of $K$, can we find elliptic curves over $K$ whose conductors are divisible only by primes in $S$? Are they finitely many? Can we find all of them?

Question 1.1 has both theoretical and computational interest. The first result is a theorem by Shavarevich which claims that the set of elliptic curves of Question 1.1 is finite (see Section 2.1). However, Shavarevich’s proof does not give a practical algorithm of computing the curves and other sophisticated ideas have to be used.

Several people have tried to make Question 1.1 explicit and compute all the curves ([CL07], [BR16], [CPV16]). However, every algorithm ends up asking for solutions of specific Diophantine equations. In the current thesis we develop a new algorithm which solves $S$–unit equations (see Section 2.6) to answer Question 1.1. In our knowledge is the first time that $S$–unit equations are directly used to compute curves with good reduction outside $S$ over a number field $K$.

Let $E$ be an elliptic curve that is an answer of Question 1.1. We also assume that $S$ contains all the primes above 2. The $\lambda$–invariant of $E$ (see Section 2.1) lies in the 2–division field $L$ of $E$. We define

$$S_L = \{ \mathfrak{B} \subset \mathcal{O}_L : \mathfrak{B} \text{ is a prime such that } \exists \mathfrak{p} \in S \text{ with } \mathfrak{B} | \mathfrak{p} \}.$$ 

We denote by $\mathcal{O}_{L,S_L}$ and $\mathcal{O}_{L,S_L}^\times$ the ring of $S_L$–integers and the group of $S_L$–units of $L$ respectively (see Section 2.2). We also denote by $K(S,6)_{12}$ the natural image
of the Selmer group $K(S,12)$ into $K(S,6)$ (see Section 2.2). We also define

$$O^*_{L,K,S_{L,1}} = \{ x \in O^*_{L,S_L} \mid \text{Norm}_{L/K}(x) = 1 \}$$

$$O^*_{L,K,S_{L,\pm 1}} = \{ x \in O^*_{L,S_L} \mid \text{Norm}_{L/K}(x) = \pm 1 \}$$

$$\mu = 1 - \lambda$$

$$j = 2^8 \left( \frac{\lambda^2 - \lambda + 1}{\lambda^2(1 - \lambda)^2} \right)^3$$

$$w = j^2(j - 1728)^3$$

The main result of this thesis is the following,

**Theorem 1.2.** Let $K$ be a number field, $S$ a finite set of prime ideals of $K$ that contains all primes above 2 and $E$ an elliptic curve over $K$ with good reduction outside $S$ with $j$–invariant equal to $j$. Then the 2–division field $L$ of $E$ is a Galois extension of $K$ unramified outside $S$ with Galois group isomorphic to a subgroup of $S_3$.

Moreover, $\lambda$ and $\mu$ are solutions of the $S$–unit equation

$$\lambda + \mu = 1$$

where $\lambda, \mu \in O^*_{L,S_L}$. When $\text{Gal}(L/K)$ is not the trivial group we can assume extra conditions for $\lambda$ and $\mu$ as follows:

- **Suppose** $\text{Gal}(L/K) = C_2$, **then** $\lambda \in O^*_{L,K,S_{L,1}}$ **and** $\mu \in O^*_{L,S_L}$.

- **Suppose** $\text{Gal}(L/K) = C_3 = \langle \sigma \rangle$, **then** $\lambda \in O^*_{L,K,S_{L,\pm 1}}$ **and** $\sigma(\lambda) = \frac{1}{\mu}$.

- **Suppose** $\text{Gal}(L/K) = S_3 = \langle \sigma, \tau \rangle$ **such that** $\sigma^3 = \tau^2 = 1$ and $\tau \sigma \tau = \sigma^{-1}$. 

3
Then \( \lambda \in \mathcal{O}_{L, \tau, S_L, \pm 1}^* \cap \mathcal{O}_{L, \sigma, S_L, 1}^* \) and \( \sigma(\lambda) = \frac{1}{\mu} \), where \( L^\tau \) and \( L^\sigma \) are the fixed fields of \( \tau \) and \( \sigma \) respectively.

Conversely, let assume that \( \text{Gal}(L/K) \) is not trivial and \( j, w, \mu \) as above. If \( \lambda \) and \( \mu \) satisfy the above conditions, according to the structure of \( \text{Gal}(L/K) \), then \( j \in \mathcal{O}_{K, S} \). Moreover, if \( w \in K(S, 6)_{12} \) then \( j \) is the \( j \)-invariant of an elliptic curve with good reduction outside \( S \cup \{ p \in \mathcal{O}_K : p \mid 3 \} \).

Theorem 1.2 is the main ingredient of the new algorithm we develop in this thesis. Together with some results of Cremona and Lingham ([CL07], Section 2.7) Theorem 1.2 allows us to answer Question 1.1 explicitly.

In more details, in this thesis Chapter 2 contains the necessary background material someone needs to understand the thesis and fixes the notation. In Chapter 3 we prove the first half of Theorem 1.2 and we clearly state the main steps of the new algorithm. In Chapter 4 we prove that there are finitely many candidate 2-division fields \( L \) for \( E \) and we give an algorithm of computing them which has its own interest. We make use of Kummer theory which we have explained earlier in Chapter 2.

In Chapter 5 we prove the second half of Theorem 1.2 together with some results which allow us to reduce the number of \( S \)-unit equations we have to solve. Chapter 6 makes use of the properties \( \lambda \) and \( \mu \) according to Theorem 1.2 to develop a suitable to our problem sieve of solving \( S \)-unit equations based on and improving Wildanger’s and Smart’s ideas ([Sma99], [Wil00]). Finally, Chapter 7 contains general conclusions.

Throughout the thesis we explain each step of the new algorithm working out in detail the example \( K = \mathbb{Q} \) and \( S = \{ 2, 3, 23 \} \).
Chapter 2

Background

In this chapter we recall basic materials that are used in the thesis. We refer to the books of Silverman [Sil86] and Cohen [Coh93, Coh00] for a detailed exposition. Throughout this thesis

- $K$ is a number field,
- $S$ (or $S_K$) a finite set of prime ideals of $K$,
- $\mathcal{O}_K$ the ring of integers of $K$,
- $\mathcal{O}_K^*$ the unit group of $\mathcal{O}_K$,
- $\mathfrak{p}$ a prime ideal of $K$,
- $K_\mathfrak{p}$ the completion of $K$ with respect to $\mathfrak{p}$,
- $\mathcal{O}_{K_\mathfrak{p}}$ the ring of integers of $K_\mathfrak{p}$,
- $\mathcal{O}_{K_\mathfrak{p}}^*$ the unit group of $\mathcal{O}_{K_\mathfrak{p}}$,
- $\pi_\mathfrak{p}$ a uniformizer of $\mathcal{O}_{K_\mathfrak{p}}$,
• $k_p$ the residue field of $\mathcal{O}_{K_p}$,

• $E$(or $E/F$) an elliptic curve defined over a field $F$.

\section*{2.1 Elliptic curves}

An elliptic curve $E$ over a field $F$ is a non–singular projective curve of genus 1 with a specified basepoint $\mathcal{O}$ that is defined over $F$. By Riemann–Roch theorem, one can prove that $E$ has always a plane model with equation of the form

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3 \quad (2.1)$$

where $a_1, \cdots, a_6 \in F$, and it is called a Weierstrass equation of $E$. Here $\mathcal{O} = [0 : 1 : 0]$ and it is called the point at infinity. If $F = K$ (or $K_p$) such that $a_1, \cdots, a_6 \in \mathcal{O}_K$ (or $\mathcal{O}_{K_p}$) then (2.1) is called an integral Weierstrass equation of $E$. In general, we write the Weierstrass equation of $E$ using the non–homogeneous coordinates $x = \frac{X}{Z}$ and $y = \frac{Y}{Z}$,

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \quad (2.2)$$

In this thesis we usually denote an elliptic curve $E$ using the affine Weierstrass equation (2.2). Two different Weierstrass equations (2.2) for $E$ are related by a linear change of variables of the form

$$x = u^2x' + r, \quad y = u^3y' + su^2x' + t,$$

with $u \in F^*$ and $r, s, t \in F$. 

6
We define the quantities

\[ b_2 = a_1^2 + 4a_2, \quad b_4 = 2a_4 + a_1a_3, \quad b_6 = a_3^2 + 4a_6, \]

\[ b_8 = a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + 2a_2a_3^2 - a_4^2, \]

\[ c_4 = b_2^2 - 24b_4, \]

\[ c_6 = -b_2^3 + 36b_2b_4 - 216b_6, \]

\[ \Delta = -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6, \]

\[ j = \frac{c_4^3}{\Delta}. \]

We can easily verify the relations

\[ 4b_8 = b_2b_6 - b_4^2, \quad 1728\Delta = c_4^3 - c_6^2. \]

The quantity \( \Delta \) is called the \textit{discriminant} of the Weierstrass equation and \( j \) the \textit{j–invariant} of \( E \).

If \( \text{char}(F) \neq 2 \) then the change of variables \((x, y) \mapsto (x, \frac{1}{2}(y - a_1x - a_3))\) gives

\[ E : y^2 = 4x^3 + b_2x^2 + 2b_4x + b_6. \quad (2.3) \]

In addition, if \( \text{char}(F) \neq 3 \) then the change of variables \((x, y) \mapsto (\frac{x-3b_2}{36}, \frac{y}{108})\) to \((2.3)\) gives

\[ E : y^2 = x^3 - 27c_4x - 54c_6 \]

\( (2.4) \)

If \( \overline{F} \) denotes the separable closure of \( F \) then,
Proposition 2.1.  (i) A Weierstrass equation defines a non–singular curve if and only if \( \Delta \neq 0 \).

(ii) Two elliptic curves are isomorphic over \( F \) if and only if they have the same \( j \)–invariant.

(iii) Let \( j_0 \in F \). Then there exists an elliptic curve defined over \( F(j_0) \) whose \( j \)–invariant is equal to \( j_0 \).

Proof. See [Sil86, Proposition III.1.4].

Group law

Let \( E \) be an elliptic curve over \( F \). We define

\[
E(F) = \{ (x, y) \in F^2 : (x, y) \in E \} \cup \{ \mathcal{O} \}.
\]

One shows that \( E(F) \) can obtain the structure of an abelian group with identity element \( \mathcal{O} \). We denote by + the operator of the group law and \( nP = \underbrace{P + P + \ldots + P}_{n \text{-times}} \). If \( F \) is a number field then the following fundamental result holds.

Theorem 2.2. \( E(F) \) is finitely generated. \( E(F) \) is called the Mordell–Weil group of \( E \) over \( F \).

Proof. See [Sil86, Chapter VIII].

For a positive integer \( n \) we define the \( n \)–torsion subgroup \( E[n] \) of \( E \) to be

\[
E[n] = \{ P \in E(F) :nP = \mathcal{O} \}
\]
The following theorem holds,

**Theorem 2.3.** Let $E$ be an elliptic curve defined over $F$ and $n$ a positive integer.

- If $\text{char}(F) = 0$ or $(\text{char}(F), n) = 1$, then

  $$E[n] \simeq \frac{\mathbb{Z}}{n\mathbb{Z}} \times \frac{\mathbb{Z}}{n\mathbb{Z}}$$

- If $\text{char}(F) = p > 0$ then one of the following is true:

  (i) $E[p^e] \simeq \{O\}$ for all $e = 1, 2, 3, \cdots$

  (ii) $E[p^e] \simeq \frac{\mathbb{Z}}{p^e\mathbb{Z}}$ for all $e = 1, 2, 3, \cdots$

*Proof.* See [Sil86, Corollary III.6.4].

We define the 2–division polynomial of $E$ to be $f_{2,E}(X) = 4X^3 + b_2X^2 + 2b_4X + b_6$. An easy calculation shows that $2^4 \Delta = \Delta(f_{2,E})$.

The 2–division field $F(E[2])$ is the field extension of $F$ adjoining the three roots of $f_{2,E}$. One can show that $F(E[2])/F$ is a Galois extension and its Galois group is isomorphic to a subgroup of $S_3$.

**Isogenies**

Let $E_1$ and $E_2$ be elliptic curves. A morphism $\phi : E_1 \to E_2$ such that $\phi(\mathcal{O}_{E_1}) = \mathcal{O}_{E_2}$ is called an *isogeny*. Two curves $E_1$ and $E_2$ are called *isogenous* if there exists a isogeny from one to the other. The degree of $\phi$, denoted $\deg \phi$, is its degree as a finite map of curves. If $\text{char} F = 0$ then $\deg \phi = \#\phi^{-1}(\mathcal{O}_{E_2})$. For
each isogeny $\phi$ there is an isogeny $\hat{\phi} : E_2 \to E_1$ with the same degree $n$ such that $\phi \circ \hat{\phi} = [n]$ and $\hat{\phi} \circ \phi = [n]$. The isogeny $\hat{\phi}$ is called the dual isogeny of $\phi$.

**Example:** Assuming that $\text{char } F \neq 2$ and $a, b \in F$ such that $r = a^2 - 4b$ and $br \neq 0$. The two elliptic curves

\[
E_1 : y^2 = x^3 + ax^2 + bx \\
E_2 : Y^2 = X^3 - 2aX^2 + rX
\]

are isogenous under the isogenies,

\[
\phi : E_1 \to E_2 \quad \quad \hat{\phi} : E_2 \to E_1, \\
(x, y) \mapsto \left( \frac{y^2}{x^2}, \frac{y(b - x^2)}{x^2} \right) \\
(X, Y) \mapsto \left( \frac{Y^2}{4X^2}, \frac{Y(r - X^2)}{8X^2} \right).
\]

One can show that $\deg \phi = 2$ and $\hat{\phi}$ is the dual isogeny of $\phi$. We have $\ker \phi = \{O_{E_1}, (0, 0)\}$ and $\ker \hat{\phi} = \{O_{E_2}, (0, 0)\}$.

**Legendre form**

**Definition 2.4.** An elliptic curve is in Legendre form if its Weierstrass equation can be written as

\[y^2 = x(x - 1)(x - \lambda).\]

**Theorem 2.5.** Assume that $\text{char}(F) \neq 2, 3$.

(i) Each elliptic curve is isomorphic over $\overline{F}$ to an elliptic curve in Legendre form

\[E_\lambda : y^2 = x(x - 1)(x - \lambda)\]
for some $\lambda \in \overline{F}$ with $\lambda \neq 0, 1$.

(ii) The $j$–invariant of $E_\lambda$ is

$$j(E_\lambda) = 2^8(\lambda^2 - \lambda + 1)^3 \overline{\lambda^2(1 - \lambda)^2}.$$ 

(iii) The map

$$\overline{F} \setminus \{0, 1\} \to \overline{F}, \quad \lambda \mapsto j(E_\lambda),$$

is surjective and exactly six–to–one except above $j = 0$ and $j = 1728$, where it is two–to–one and three–to–one, respectively.

Proof. See [Sil86, Proposition III.1.7].

Let $e_1, e_2, e_3$ be the three roots of $f_{2,E}$ for an elliptic curve $E$. We define the $\lambda$–invariant $\lambda$ of $E$ to be $\lambda = \frac{e_1 - e_2}{e_1 - e_3}$. One can show that $E$ is isomorphic over $\overline{F}$ to the Legendre elliptic curve $E_\lambda$.

Even though we define $\lambda$–invariant using the roots of $f_{2,E}$ which depend on the model we have chosen, Theorem 2.5 says that $\lambda$ is independent of the model of $E$. Moreover, one can show that $\lambda$ is divisible only by primes that divide $2N_E$, where $N_E$ is the conductor of $E$ (see Chapter 3).

Remark: Every element of the set $\Lambda := \{\lambda, 1 - \lambda, \frac{1}{\lambda}, \frac{1}{1-\lambda}, \frac{\lambda}{\lambda-1}, 1 - \frac{1}{\lambda}\}$ maps to the same $j$–invariant under the above map and so $E$ is isomorphic over $\overline{F}$ to $E_t$ for every $t \in \Lambda$. By the definition of $\lambda$ we understand that $F(E[2]) \supseteq F(\lambda)$.
Minimal discriminant

Let $E$ be an elliptic curve over a number field $K$ and $\mathfrak{p}$ a prime ideal of $K$. By the natural embedding of $K$ to $K_\mathfrak{p}$ we can see that $E$ is also defined over $K_\mathfrak{p}$. For an integral Weierstrass equation of $E$ over $K_\mathfrak{p}$ with discriminant $\Delta_{K_\mathfrak{p}}$ we have $v_\mathfrak{p}(\Delta_{K_\mathfrak{p}}) \geq 0$. So, $v_\mathfrak{p}(\Delta_{K_\mathfrak{p}})$ has a minimal value among all the integral Weierstrass models of $E$ over $K_\mathfrak{p}$. We say that a Weierstrass equation for $E$ over $K$ is minimal at $\mathfrak{p}$ if it is integral as a curve over $\mathfrak{p} K_\mathfrak{p}$ and $v_\mathfrak{p}(\Delta)$ is minimal. The minimal value of $v_\mathfrak{p}(\Delta)$ is called the valuation of the minimal discriminant of $E$ at $\mathfrak{p}$.

**Proposition 2.6.** (i) Every elliptic curve $E/K_\mathfrak{p}$ has a minimal Weierstrass equation.

(ii) A minimal Weierstrass equation of $E/K_\mathfrak{p}$ is unique up to a change of variables with $u \in \mathcal{O}_{K_\mathfrak{p}}^*$ and $r, s, t \in \mathcal{O}_{K_\mathfrak{p}}$.

**Proof.** See [Sil86, Proposition VII.1.3].

Having chosen a minimal Weierstrass equation of $E$ at $\mathfrak{p}$ we can reduce the coefficients mod $\mathfrak{p}$ and get a curve $E_\mathfrak{p}$ over $k_\mathfrak{p}$. If the valuation of the minimal discriminant of $E$ at $\mathfrak{p}$ is zero then the curve $E_\mathfrak{p}$ is nonsingular, so an elliptic curve over $k_\mathfrak{p}$. In this case we say that $E$ has good reduction at $\mathfrak{p}$, otherwise bad reduction at $\mathfrak{p}$.

Let $M_0^0_K$ be the set of prime ideals of $K$. If $\Delta_\mathfrak{p}$ is the discriminant of a minimal Weierstrass model of $E$ over $K$ at $\mathfrak{p}$, then the minimal discriminant $\mathcal{D}_{E/K}$ of $E$ over $K$ is the ideal $\prod_{\mathfrak{p} \in M_0^0_K} \mathfrak{p}^{v_\mathfrak{p}(\Delta_\mathfrak{p})}$. Fixing a Weierstrass model of $E$ over $K$ with

1It is important to mention that we are always able to find a minimal Weierstrass model of $E$ at $\mathfrak{p}$ with $a_i \in \mathcal{O}_K$. 

12
discriminant $\Delta$, there exists $u_p \in K$ for each $p \in \mathcal{M}_K^0$ such that $\Delta = u_p^{12} \Delta_p$. If we define $a_\Delta = \prod_{p \in \mathcal{M}_K^0} p^{-\nu_p(u_p)}$ then it holds

$$D_{E/K} = (\Delta) a_\Delta^{12}.$$ 

One can show that the ideal class $\overline{a}_{E/K}$ of $a_\Delta$ is independent of the Weierstrass model for $E$ and $\overline{a}_{E/K}$ is called the Weierstrass class of $E$ over $K$. A global minimal Weierstrass model for $E$ over $K$ is a Weierstrass integral model of $E$ over $K$ such that $D_{E/K} = (\Delta)$.

**Proposition 2.7.** There exists a global minimal Weierstrass model for $E$ over $K$ if and only if $\overline{a}_{E/K} = (1)$.

*Proof.* See [Sil86, Proposition VIII.8.2].

Even though we are not always able to find a global minimal model for $E$, we are able to find an integral model that is minimal at each fixed prime $p$ (Tate’s algorithm [Sil94, IV §9]).

Let $K$ be a number field and $S$ a finite set of prime ideals of $K$. We say that an elliptic curve $E$ over $K$ has good reduction outside $S$ if it has good reduction at all primes not in $S$. The following classical result due to Shafarevich holds.

**Theorem 2.8** (Shafarevich). Let $K$ be a number field and $S$ a finite set of prime ideals of $K$. Then up to isomorphism over $K$, there are only finitely many elliptic curves $E$ over $K$ which have good reduction outside $S$.

*Proof.* See [Sil86, Theorem IX.6.1].
We denote by $\mathcal{E}_{K,S}$ the set of curves that Theorem 2.8 describes. Unfortunately, the proof of Shafarevich’s theorem cannot be translated in an algorithm that computes $\mathcal{E}_{K,S}$. The goal of this thesis is to make the above theorem explicit.

Isogenous curves have the same set of bad primes.

**Proposition 2.9.** Let $E_1/K$ and $E_2/K$ be two isogenous over $K$ elliptic curves. Then $E_1$ has good reduction at $p$ if and only if $E_2$ has good reduction at $p$.

*Proof.* See [Sil86, Corollary VII.7.2].

**Twists**

Let $E$ be an elliptic curve over $K$. A *twist* of $E$ is an elliptic curve $E'/K$ that is isomorphic to $E$ over $\overline{K}$. The set of twists of $E$, modulo $K$–isomorphisms, is denoted by $\text{Twist}((E, \mathcal{O})/K)$.

Let $E$ be an elliptic curve over $K$ of the form $y^2 = x^3 + a_2x^2 + a_4x + a_6$ and $d \in K^\times$. We denote by $E^{(d)}$ the elliptic curve given by

$$E^{(d)} : y^2 = x^3 + a_2 dx^2 + a_4 d^2 x + d^3 a_6$$

and it is called the *twist* of $E$ by $d$. Note that $j(E^{(d)}) = j(E)$ and $\Delta(E^{(d)}) = d^6 \Delta(E)$. We can explicitly describe $\text{Twist}((E, \mathcal{O})/K)$.

**Proposition 2.10.** Let

$$n = \begin{cases} 2, & \text{if } j \neq 0, 1728, \\ 4, & \text{if } j = 1728, \\ 6, & \text{if } j = 0. \end{cases}$$
Then Twist \(((E, \mathcal{O})/K)\) is canonically isomorphic to \(K^*/K^{*n}\).

More precisely, if \(E\) is given in the Weierstrass form

\[
E : y^2 = x^3 + Ax + B
\]

and \(d \in K^*\), then the element \(d\mod K^{*n}\) corresponds to the curve with Weierstrass equation

1. \((i)\) \(y^2 = x^3 + d^2Ax + d^3B\) if \(j \neq 0, 1728\),
2. \((ii)\) \(y^2 = x^3 + dAx\) if \(j = 1728\),
3. \((iii)\) \(y^2 = x^3 + dB\) if \(j = 0\).

Proof. See [Sil86, Proposition X.5.4].

---

**S–integral points**

Let \(K\) be a number field, \(S\) a finite set of prime ideals of \(K\) and \(E\) an elliptic curve over \(K\). A point \(P = (x, y)\) on \(E(K)\) is called S–integral if \(x, y \in \mathcal{O}_{K,S}\). If \(S = \emptyset\) then \(P\) is called integral point.

**Theorem 2.11** (Siegel). Let \(K\) be a number field, \(S\) a finite set of prime ideals of \(K\) and \(E\) an elliptic curve over \(K\). The set of S–integral points of \(E(K)\) is finite.

Proof. See [Sil86, Corollary IX.3.2.1].

---

\(^2\)See Section 2.2 for the definition of \(\mathcal{O}_{K,S}\).
2.2 Number fields

2.2.1 \( S \)–properties

Let \( K \) be a number field and \( S \) a finite set of prime ideals of \( K \). We define the ring of \( S \)–integers and the group of \( S \)–units of \( K \) to be

\[
\mathcal{O}_{K,S} = \{ x \in K : v_p(x) \geq 0, \forall p \not\in S \}
\]

\[
\mathcal{O}_{K,S}^* = \{ x \in K : v_p(x) = 0, \forall p \not\in S \}
\]

We observe that \( \mathcal{O}_{K,S}^* \) is the group of units for \( \mathcal{O}_{K,S} \). One can show that \( \mathcal{O}_{K,S} \) is a Dedekind domain and \( \mathcal{O}_{K,S}^* \) is a finitely generated abelian group. The generators of \( \mathcal{O}_{K,S}^* \) can be chosen to be algebraic integers and \( \mathcal{O}_{K,S}^* \) decomposes as

\[
\mathcal{O}_{K,S}^* = \mathcal{O}_{K}^* \bigoplus \bigoplus_{i=1}^{\#S} \mathbb{Z} \gamma_i
\]  

(2.6)

where \( \gamma_i \notin \mathcal{O}_{K}^* \).

We say that an ideal \( I \) of \( K \) is \( S \)–integral if \( v_p(I) \geq 0 \) for all \( p \not\in S \). We define the \( S \)–class group \( C\ell_S(K) \) of \( K \) and \( S \) to be the class group of \( \mathcal{O}_{K,S} \).

**Proposition 2.12.** There is a canonical isomorphism

\[
C\ell_S(K) \simeq C\ell(K)/\langle \overline{p} \rangle_{p \in S}
\]

where \( \langle \overline{p} \rangle \) is the subgroup of \( C\ell(K) \) generated by the images of \( p \) in \( C\ell(K) \).

**Proof.** See [Coh00, Proposition 7.4.4]. \( \square \)

For a positive natural integer \( n \) we define the \( n \)–Selmer group of \( K \) and \( S \) to
be
\[ K(S, n) = \{ x \in K^*/K^{*n} : v_p(x) \equiv 0 \mod n, \forall p \not\in S \}. \]

The \( n \)-Kummer exact sequence of \( \mathcal{O}_{K,S}^* \) holds:

\[ 1 \to \mathcal{O}_{K,S}^*/\mathcal{O}_{K,S}^{*n} \to K(S, n) \xrightarrow{\alpha_n} \text{Cl}_S(K)[n] \to 1 \]

where \( \text{Cl}_S(K)[n] \) is the \( n \)-torsion subgroup of \( \text{Cl}_S(K) \) and the map \( \alpha_n : K(S, n) \to \text{Cl}_S(K)[n] \) is given by \( x \mapsto [I_S] \) such that \( (x)\mathcal{O}_{K,S} = I_S^n \).

**Proposition 2.13.** Let \( m, n \) be two coprime positive integers. Then

\[ K(S, mn) \simeq K(S, m) \times K(S, n) \]

under the identity map and inverse \((u, v) \mapsto v^{am}w^{bn} \) such that \( am + bn = 1 \).

**Proof.** See [CL07, Proposition 2.1]. \( \square \)

For positive integers \( m, n \) we denote by \( K(S, m)_mn \) the image of the natural map \( K(S, mn) \to K(S, m) \).

For an extension \( L/K \) of number fields and a set \( S_L \) of prime ideals of \( L \) we define

\[ \mathcal{O}_{L,K,S_L,1}^* = \{ x \in \mathcal{O}_{L,S_L}^* | \text{Norm}_{L/K}(x) = 1 \} \]
\[ \mathcal{O}_{L,K,S_L,\pm1}^* = \{ x \in \mathcal{O}_{L,S_L}^* | \text{Norm}_{L/K}(x) = \pm1 \} \]
Finally, for a place \( p \) of \( K \) we define its absolute value to be,

\[
|x|_p = \begin{cases} 
p^{-f_p v_p(x)}, & \text{if } p \text{ is a finite prime.} 
\mid \sigma_p(x) \mid, & \text{if } p \text{ is an infinite real prime.} 
\mid \sigma_p(x) \mid^2, & \text{if } p \text{ is an infinite complex prime.} 
\end{cases}
\]

where \( \sigma_p \) is the associated embedding into \( \mathbb{R} \) or \( \mathbb{C} \) when \( p \) is an infinite place and \( f_p \) is the residual degree and \( p \) the rational prime below \( p \) when \( p \) is a finite prime.

### 2.2.2 Hilbert symbol

In this paragraph we present the basic properties of Hilbert symbol without getting into the details (see [Neu99] for a good exposition of the topic).

Let \( F \) be a local field or \( \mathbb{R}, \mathbb{C} \) and \( n \) a positive integer. We also assume that \( \mu_n \subset F^* \), where \( \mu_n \) is the group of the \( n \)-th roots of unity of \( F \). The general Hilbert symbol of \( F \) with respect to \( n \) is a nondegenerate bilinear pairing

\[
\left( \frac{a}{F} \right)_n : F^*/F^{*n} \times F^*/F^{*n} \rightarrow \mu_n.
\]

We skip the index when \( n = 2 \) and we simply call it Hilbert symbol of \( F \).

The general Hilbert symbol has some fundamental properties:

**Proposition 2.14.** Let \( a, b, c \in F^* \). Then,

(i) \( \left( \frac{a b c}{F} \right)_n = \left( \frac{a c}{F} \right)_n \left( \frac{b c}{F} \right)_n \).

(ii) \( \left( \frac{a b c}{F} \right)_n = \left( \frac{a b}{F} \right)_n \left( \frac{a c}{F} \right)_n \).

(iii) \( \left( \frac{a b}{F} \right)_n = 1 \iff a \text{ is a norm for the extension } F(\sqrt[n]{b})/F. \)
(iv) \((\frac{a,b}{F})_n = (\frac{b,a}{F})^{-1}_n\).

(v) \((\frac{a_1-a}{F})_n = 1\) and \((\frac{a-a}{F})_n = 1\).

(vi) if \((\frac{a,b}{F})_n = 1\) for all \(b \in F^\times\) then \(a \in F^{*n}\).

**Proof.** See [Neu99, Proposition V.3.2].

The Hilbert symbol of \(F, n = 2\), can also be defined by

\[
\left(\frac{a,b}{F}\right) = \begin{cases} 
1, & \text{if } z^2 = ay^2 + bx^2 \text{ has a solution in } \mathbb{P}^2(F) \\
-1, & \text{otherwise.}
\end{cases}
\]

The natural embedding of \(K \hookrightarrow K_p\) allows us to define general Hilbert symbol of \(K\) with respect to \(p\) and \(n\).

For a number field \(K\) we define the map \((\frac{\cdot}{K}) : K^\times/K^\times 2 \times K^\times/K^\times 2 \to \mu_2\) such that \((\frac{a,b}{K}) = 1\) if \(z^2 = ay^2 + bx^2\) has a solution in \(\mathbb{P}^2(K)\), otherwise \(-1\). Even though the above map is not a symbol, because it is not bilinear, we call it (global) Hilbert symbol of \(K\).

### 2.2.3 More results

Let \(K\) be a number field. A useful result that we use later in Chapter 4 is the following,

**Proposition 2.15.** Let \(K\) be a number field and \(f\) an irreducible polynomial over \(K\) of degree \(n\). If \(K(f)\) is the splitting field of \(f\) then \(\text{Gal}(K(f)/K) \subset A_n\) if and only if \(\Delta(f)\) is a square in \(K\).

**Proof.** See [Coh93, Proposition 6.3.1].
Let \( G = \langle g_0, g_1, \ldots, g_n \rangle \) be a finitely generated subgroup of \( K^* \) and \( \mathfrak{p} \) a prime ideal of \( K \). Let \( g \in G \) such that \( g = \prod_{i=0}^{n} g_i^{x_i} \) with \( |x_i| \leq b_i \) for \( i = 0, 1, \ldots, n \) where \( b_i \) are positive integers.

**Lemma 2.16.** With the above notation there exists a finite set of elements \( \mu_i \in K \) for \( i = 0, 1, \ldots, s_n \) such that

(i) \( \text{ord}_{\mathfrak{p}}(\mu_i) = 0 \).

(ii) \( s_n = n \) if \( \text{ord}_{\mathfrak{p}}(g_i) = 0 \) for all \( i = 0, 1, \ldots, n \) otherwise \( s_n = n - 1 \).

(iii) There are integers \( y_i \) with \( |y_i| \leq |x_i| \leq b_i \) such that

\[
g = \mu_0 \prod_{i=1}^{s_n} \mu_i^{y_i}.
\]

**Proof.** See [Sma98, Lemma IX.3]. \( \square \)

### 2.3 \( p \)-adic analysis

Let \( \mathfrak{p} \) be a prime ideal of a number field \( K \), \( p \) the rational prime below \( \mathfrak{p} \) and \( e_p \) and \( f_p \) the ramification and residual degree of \( \mathfrak{p} \). Let \( q = p^{f_p} \). For an element \( x \in K_p \) we define

\[
\text{ord}_p(x) = \frac{\text{ord}_p(x)}{e_p}.
\]

With respect to \( \text{ord}_p(\cdot) \) we define

\[
|x|_p = p^{-\text{ord}_p(x)}.
\]
The absolute value $|\cdot|_p$ is global in the sense that has the same value if we consider $x$ as an element of a finite extension $L_p$ of $K_p$.

For an element $x \in K_p$ such that $|x - 1|_p < 1$, we define the $p$-adic logarithm by

$$\log_p(x) = -\sum_{i=1}^{\infty} \frac{(1 - x)^i}{i}.$$ 

We can extend the above definition for all element $x \in K_p$ such that $|x|_p = 1$ in the following way. Let $o$ be the multiplicative order of $x$ modulo $p$. We choose $t$ such that $p^t > e_p$ then one can show that $\text{ord}_p(1 - x^{op^t}) > 1$. Thus we define

$$\log_p(x) = \frac{1}{op^t} \log_p(x^{op^t}) = -\frac{1}{op^t} \sum_{i=1}^{\infty} \frac{(1 - x^{op^t})^i}{i}.$$ 

Then $\log_p$ satisfies the usual property. For $x, y \in K_p$ such that $|x|_p = |y|_p = 1$, we have $\log_p(xy) = \log_p(x) + \log_p(y)$. For an element $x$ that satisfies $|x|_p < p^{-\frac{1}{e_p - 1}}$, it also holds

$$\text{ord}_p \left( \log_p(1 + x) \right) = \text{ord}_p x.$$ 

For more details about $p$-adic analysis see [Sma98, Chapter II].

### 2.4 Kummer theory

Let $K$ be a number field. An extension $L/K$ is called abelian if $L/K$ is Galois and its Galois group $\text{Gal}(L/K)$ is an abelian group. If $\text{Gal}(L/K)$ is a cyclic group then the extension is called cyclic. In this section we explicitly describe all cyclic extensions of $K$ of prime degree $\ell$, and those which are unramified outside a given set of prime ideals $S$ of $K$. 

21
The case $\zeta_n \in K$

Let $K$ be a number field and $\zeta_n$ a primitive $n$–th root of unity such that $\zeta_n \in K$. Kummer theory gives a description of the abelian Galois extensions of $K$ with exponent dividing $n$.

**Theorem 2.17** (Kummer). Let $K$ be a number field such that $\zeta_n \in K$ for $n$ a positive integer. If $K_n$ is the maximal abelian extension of $K$ of exponent $n$ and $G_K = \text{Gal}(\overline{K}/K)$ the Galois group of the algebraic closure of $K$ then

$$\text{Hom}(\text{Gal}(K_n/K), \mu_n) \simeq H^1(G_K, \mu_n) \simeq K^*/K^{*n}.$$  

**Proof.** See [NSW08, Theorem 6.2.2] $\square$

An immediate consequence of the above theorem is the following proposition.

**Proposition 2.18.** Let $B$ be a finite subgroup of $K^*/K^{*n}$. The map $B \mapsto L = K(\sqrt[n]{B})$, where $K(\sqrt[n]{B})$ is the Galois extension of $K$ adjoining the $n$–th roots of all elements of $B$, is a bijection between the finite subgroups of $K^*/K^{*n}$ and finite abelian extensions of $K$ with exponent dividing $n$. Moreover,

(i) An extension $L/K$ is a cyclic extension of degree $n$ if and only if there exists $a \in K^*$ such that $a$ is exactly of order $n$ in $K^*/K^{*n}$ and $L = K(\sqrt[n]{a})$.

(ii) The two cyclic extensions $L_1 = K(\sqrt[n]{a_1})$ and $L_2 = K(\sqrt[n]{a_2})$ are $K$–isomorphic if and only if there exists an integer $j$ coprime to $n$ and $\gamma \in K^*$ such that $a_2 = a_1^j \gamma^n$.

**Proof.** Use Theorem 2.17 or see [Coh00, Theorem 10.2.5, Corollary 10.2.7]. $\square$
Since an abelian Galois extension is a tower of abelian Galois extensions of prime degree, for the rest of the section we work on the case \( n = \ell \) be a prime. We really care to describe Galois extensions of \( K \) with prime degree whose relative discriminant is not divisible by primes outside a finite set of primes \( S \) of \( K \).

**Proposition 2.19.** Let \( K \) be a number field, \( \ell \) a prime number such that \( \zeta_\ell \in K \) and \( L = K(\sqrt[\ell]{a}) \), where \( a \in K^* \setminus K^{*\ell} \). For a prime ideal \( \mathfrak{p} \) of \( \mathcal{O}_K \) we define \( z(\mathfrak{p}, \ell) = \ell v_\mathfrak{p}(1 - \zeta_\ell) + 1 \). Then \( \mathfrak{p} \) is unramified in \( L/K \) if and only if \( \ell | v_\mathfrak{p}(a) \), and in addition, either \( \mathfrak{p} \nmid \ell \) or \( \mathfrak{p} | \ell \) and the congruence

\[
x^\ell \equiv a \pmod{\mathfrak{p}^{z(\mathfrak{p}, \ell) - 1 + v_\mathfrak{p}(a)}}
\]

has a solution in \( K \).

**Proof.** See [Coh00, Corollary 10.2.12]. \( \square \)

**Corollary 2.20.** Let \( K \) be a number field, \( \ell \) a prime number such that \( \zeta_\ell \in K \), \( L = K(\sqrt[\ell]{a}) \), where \( a \in K^* \setminus K^{*\ell} \) and \( S \) a finite set of primes ideals of \( \mathcal{O}_K \). If \( L/K \) is unramified outside \( S \) then \( a \in K(S, \ell) \).

**Proof.** By Proposition 2.19 and the definition of \( K(S, \ell) \). \( \square \)

**The case \( \zeta_n \not\in K \)**

The situation is more complicated when \( \zeta_n \not\in K \). We have to adjoin \( \zeta_n \) in \( K \) to get an extension \( K_z = K(\zeta_n) \). Using Kummer theory we find a cyclic extension \( L_z \) of \( K_z \) of degree \( n \) with suitable properties. Then we go down to the desired extension \( L \). Again we care only for the case \( n = \ell \), an odd prime. Because of the necessity to work with \( K_z \) and \( L_z \) we state the following proposition.
Proposition 2.21. Let $L$ be a number field and $L_1$ and $L_2$ two abelian extensions of $L$ with Galois groups $G_1$ and $G_2$, respectively. Then the compositum $L_1L_2$ of $L_1$ and $L_2$ is an abelian extension of $L$, and $G_1$ and $G_2$ can be identified with subgroups of $\text{Gal}(L_1L_2/L_2)$ and $\text{Gal}(L_1L_2/L_1)$, respectively. Moreover, $G_1 \simeq \text{Gal}(L_1L_2/L_2)$ if and only if $L_1 \cap L_2 = L$.

Proof. See [Coh00, Proposition 5.3.1].

Let $g_0$ be a primitive root mod $\ell$. Then the following proposition gives all the necessary information about the extension $K_z$.

Proposition 2.22. The extension $K_z/K$ is a cyclic extension of degree $d = \frac{\ell - 1}{m}$ for some divisor $m$ of $\ell - 1$ with $m < \ell - 1$. The Galois group $G_{K_z} = \text{Gal}(K_z/K)$ is generated by the automorphism $\tau$ with order $d$ which is defined by $\tau(\zeta_\ell) = \zeta_\ell^g$ and $\tau(x) = x$ for $x \in K$, where $g = g_0^m$.

Proof. See [Coh00, Proposition 5.3.2].

Let $W$ be an $\mathbb{F}_\ell$-vector space together with an action of $G_{K_z}$. For the rest of the section, the abelian group law of $W$ is written multiplicatively.

Then $\tau$ acts as an endomorphism $t$ of $W$, of order dividing $d$. Since $d | (\ell - 1)$ hence is coprime to $\ell$, $X^d - 1$ is squarefree polynomial in $\mathbb{F}_\ell[X]$, hence $t$ is diagonalizable. Moreover, the eigenvalues of $t$ are among of the roots of $X^d - 1$, hence are among the elements of $\mathbb{F}_\ell^*$ which are roots of this polynomial, these are powers of $g = g_0^m$. By linear algebra we know that $W = \oplus_{0 \leq k < d} W_k$, where $W_k$ is the eigenspace corresponding to the eigenvalue $g^k$ of $\tau$. 
For $0 \leq k < d$ we define,

$$e_k = \frac{1}{d} \sum_{0 \leq a < d} g^{-ka} = -m \sum_{0 \leq a < d} g^{-ka} \in \mathbb{F}_\ell[G_{K_z}] .$$

**Proposition 2.23.** The eigenspace $W_k$ is equal to $e_k W = \{ x^{e_k} \mid x \in W \}$.

**Proof.** See [Coh00, Corollary 5.3.4]

Now we are in position to present the main theorem in the case $\zeta_\ell \not\in K$ with $W = K^*_z/K^*_z$.

**Theorem 2.24.** Let $K$ be a number field and $L$ an abelian extension of $K$ of degree $\ell$. Assume that $\zeta_\ell \not\in K$, $K_z = K(\zeta_\ell)$ and $L_z = L(\zeta_\ell)$. Let $g_0$ be a primitive root modulo $\ell$, $d = [K_z : K] = \frac{\ell - 1}{m}$ and $g = g_0^m$ as above. Finally, let $W = K^*_z/K^*_z$.

(i) Any element $a \in K_z$ such that $L_z = K_z(\sqrt[\ell]{a})$ belong to the eigenspace $W_1$ of $W$.

(ii) If $L_z = K_z(\theta)$ with $\theta = \sqrt[\ell]{a}$ as in (i), then $L = K(\eta)$ with

$$\eta = \text{Tr}_{L_z/L}(\theta) = \sum_{0 \leq i < d} \tau^i(\theta)$$

where $\tau$ is any extension to $L_z$ of the $K$–automorphism $\tau$ of $K_z$.

(iii) A defining polynomial for $L/K$ is given by the polynomial

$$P(X) = \prod_{0 \leq j < \ell} \left( X - \sum_{0 \leq i < d} \zeta_\ell^{jg^i} \tau^i(\theta) \right) \in K[X].$$

25
(iv) We have

\[ \theta = \frac{1}{\ell} \sum_{0 \leq j < \ell} \zeta_{\ell}^{-j} \sigma^j(\eta). \]

(v) Conversely, if we are given a abelian extension \( L \) of \( K \) of prime degree \( \ell \) by \( L = K(\eta) \) and if we define \( \theta \) by the above formula, then \( a = \theta^\ell \in K(\ell) \) and \( a \in W_1 \).

Proof. See [Coh00, Theorem 5.3.5].

Even though Theorem 2.24 gives a defining polynomial for \( L/K \), we need to know an extension of \( \tau \) to \( L_z/K \). We define \( \lambda \) by the above formula, then \( a = \lambda^\ell \in K(\ell) \) and \( a \in W_1 \).

Proposition 2.25. Let \( a \in K_z^* \) such that \( \tau(a) = a^g \gamma^\ell \) for some \( \gamma \in K_z^* \). Then \( a = \beta^\lambda \delta^\ell \), where

\[ \beta = \gamma^{-\xi} \zeta_{\ell}^k \text{ with } \xi = \left( \frac{g^d - 1}{\ell} \right)^{-1} \text{ mod } \ell \]

for some integer \( k \) and some \( \delta \in K_z^* \).

Conversely, let \( \beta \) be given such that \( a = \beta^\lambda \) and let \( \lambda = \lambda_0 + \nu \ell \) for \( \nu \in \mathbb{Z}[G_z] \) and \( \lambda_0 \) as above. Then \( \tau(a) = a^g \gamma^\ell \) with \( \gamma = \beta^\mu \) and \( \mu = -\frac{g^d - 1}{\ell} + (\tau - g)\nu \).

Proof. See [Coh00, Proposition 5.3.6].
Corollary 2.26. Keep the notation of Theorem 2.24 and Proposition 2.25. Then if \( a = \beta \lambda \), we can take \( \tau(\theta) = \theta^a \beta^\mu \).

Proof. See \[Coh00, Corollary 5.3.7\].

Example: Let assume that \( \ell = 3 \). Then we have that \( d = 2, m = 1, g_0 = g = 2, \lambda = \lambda_0 = e_1 = 2 + \tau, \nu = 0 \) and \( \xi = -1 \). By Theorem 2.24 we know that \( a \in W_1 \), so \( a = \beta^4 \delta^3 \) for some \( \delta \in K_2^\ast \). If \( \delta = 1 \) Corollary 2.26 says that \( \tau(\theta) = \theta^2 \beta^6 = \frac{\beta^2}{\beta} \) and by Theorem 2.24 we have a defining polynomial of \( L/K \) to be

\[
P(X) = X^3 - 3eX - e \text{Tr}_{K_2/K}(\beta)
\]

where \( e = \text{Norm}_{K_2/K}(\beta) \).

2.5 Lattices

Let \( n \) be a positive integer. A lattice \( L \) in \( \mathbb{R}^n \) is a \( \mathbb{Z} \)-module spanned by \( n \) linearly independent vectors. The set of linearly independent vectors is called a basis of \( L \). Formally \( L \) is of the form

\[
L = \left\{ \sum_{i=1}^{n} x_i \vec{b}_i : x_i \in \mathbb{Z} \right\}
\]

where the vectors \( \vec{b}_1, \ldots, \vec{b}_n \) are a basis for \( L \). We denote by \( B \) the matrix with columns \( \vec{b}_i, i = 1, \ldots, n \).

We denote by \( \langle , \rangle \) the usual euclidean inner product of \( \mathbb{R}^n \). The following theorem holds,
Theorem 2.27 (Gram–Schmidt). A vector space with basis $\vec{b}_1, \ldots, \vec{b}_n$ and inner product $\langle , \rangle$ has an orthogonal basis given by $\vec{b}_1^*, \ldots, \vec{b}_n^*$ where

$$\vec{b}_i^* = \vec{b}_i - \sum_{j=1}^{i-1} \mu_{i,j} \vec{b}_j^*, \quad i = 1, \ldots, n,$$

where the $\mu_{i,j}$ are given by

$$\mu_{i,j} = \frac{\langle \vec{b}_i, \vec{b}_j^* \rangle}{\langle \vec{b}_j^*, \vec{b}_j^* \rangle}.$$

A powerful tool in lattices and computational number theory is LLL–algorithm. In the next lines we give a brief exposition of some of its properties (see [LLL82] or [Sma98, chapter V]). We call a basis $B$ of a lattice LLL–reduced if the associated Gram–Schimdt basis $B^*$ satisfies

(i) $|\mu_{i,j}| \leq \frac{1}{2}, 1 \leq j < i \leq n,$

(ii) $\|\vec{b}_i^* + \mu_{i,i-1} \vec{b}_{i-1}^*\|^2 \geq \frac{3}{4} \|\vec{b}_{i-1}^*\|^2, \quad 1 < i \leq n$

Such a basis always exists and a quick algorithm of computing it is given in [LLL82]. A LLL–reduced basis has a lot of very nice properties. For a lattice $\mathcal{L}$ and a vector $\vec{y} \in \mathbb{R}^n$ we denote

$$\ell(\mathcal{L}, \vec{y}) = \begin{cases} 
\min_{\vec{v} \in \mathcal{L}} \|\vec{v} - \vec{y}\|, & \text{if } \vec{y} \notin \mathcal{L}, \\
\min_{0 \neq \vec{v} \in \mathcal{L}} \|\vec{v}\|, & \text{if } \vec{y} \in \mathcal{L}.
\end{cases}$$

Theorem 2.28. Let $B$ be a LLL–reduced basis for a lattice $\mathcal{L}$. For all $\vec{v} \neq 0$ in $\mathcal{L}$ it holds

$$\|\vec{b}_1\|^2 \leq c_1 \|\vec{v}\|^2,$$
where \( c_1 = \max \left\{ \frac{\|\vec{b}_1\|^2}{\|\vec{b}_i\|^2} : 1 \leq i \leq n \right\} \).

Proof. See [Sma98, Theorem V.9]. \( \square \)

Let \( \vec{y} \in \mathbb{R}^n \) such that \( \vec{y} \notin \mathcal{L} \). Let \( B \) be an LLL-reduced basis for \( \mathcal{L} \). We define \( \vec{\phi} = B^{-1} \vec{y} \). We denote by \([\cdot]\) the nearest integer function.

**Theorem 2.29.** Let \( i_0 \) be the largest index such that \([\phi_{i_0}] \neq 0\). Then for all \( \vec{v} \in \mathcal{L} \) it holds
\[
\|\vec{v} - \vec{y}\|^2 \geq c_1^{-1} \cdot [\phi_{i_0}] \cdot \|\vec{b}_1\|^2,
\]
where \( c_1 \) is defined in Theorem 2.28.

Proof. See [Sma98, Theorem V.10]. \( \square \)

The above theorems can be used to get a lower bound for \( \ell(\mathcal{L}, \vec{y}) \). We have to mention that we can use \( c_1 = 2^{n-1} \).

### 2.6 \( S \)-unit equation

Let \( K \) be a number field and \( G_1, G_2 \) two finitely generated subgroups of \( K^* \). We call \( S \)-unit equation the Diophantine equation of the form
\[
ax + by = 1 \quad (2.7)
\]
where \((x, y) \in G_1 \times G_2\) and \(a, b\) are fixed elements of \( K^* \).

**Theorem 2.30.** Let \( K \) be a number field and \( S \) a finite set of prime ideals of \( K \). If \( a, b \in K^* \) then the \( S \)-unit equation
\[
ax + by = 1
\]
has finitely many solutions \((x, y)\) where \(x, y \in \mathcal{O}_{K,S}^*\). The number of solutions is at most \(3 \cdot 7^{[K:\mathbb{Q}]} + 2^\#S\).

**Proof.** See [Sil86, Theorem IX.4.1] and [Eve84].

Since the equation (2.7) plays an important role in number theory with many applications, it has been studied a lot. Many methods of solving \(S\)–unit equations algorithmically have been developed, starting with De Weger’s thesis work where he gave an algorithmic solution for the special case \(K = \mathbb{Q}\) using lattice approximation reduction algorithms ([Weg87], [Weg88]). Many others used and extended De Weger’s idea to solve \(S\)–unit equations over an arbitrary number field ([TdW89], [Sma95], [TW92], [Sma98], [EG16]).

### 2.7 Cremona–Lingham method

Let \(K\) be a number field and \(S\) a finite set of prime ideals of \(K\). In this section we briefly explain Cremona–Lingham method ([CL07]) which is an algorithm that computes \(E_{K,S}\).

Cremona and Lingham show that for computing \(E_{K,S}\) it is enough to determine the \(j\)–invariant of the curves in \(E_{K,S}\). Given \(j\) they explicitly construct\(^3\) an elliptic curve \(E\) over \(K\) with good reduction outside \(S\) and \(j\)–invariant equal to \(j\). Then by twisting they compute all the curves of \(E_{K,S}\).

Since we want to explicitly find models of curves, it is necessary to find criteria, based on invariants of the model, that tell us when a model of a curve \(E\) has good reduction at a prime \(p\) and good reduction outside \(S\).

\(^3\)If it is possible.
Proposition 2.31. Let $E$ be an elliptic curve over a number field $K$ with good reduction at $p$. Then for any Weierstrass model of $E$, with invariants $c_4, c_6, \Delta$, there exists an integer $e$ such that

$$\text{ord}_p(\Delta) = 12e, \quad \text{ord}_p(c_4) \geq 4e, \quad \text{ord}_p(c_6) \geq 6e.$$  

In addition, if $\text{ord}_p(6) = 0$ then the above condition is sufficient.

Proof. See [CL07, Lemma 3.1].

Let assume that $j \neq 0, 1728$. We define $S^{(n)} = S \cup \{p : p | n\}$.

Proposition 2.32. Let $E$ be an elliptic curve over $K$ with good reduction outside $S$ and $j(E) = j$. Let $w = j^2(j - 1728)^3$. Then

$$\Delta \in K(S, 12), \quad j \in \mathcal{O}_{K,S}, \quad w \in K(S, 6)_{12}.$$  

Conversely, if $j \in \mathcal{O}_{K,S}$ with $w \in K(S, 6)_{12}$ then there exist elliptic curves $E$ with $j(E) = j$ and good reduction outside $S^{(6)}$.

Proof. See [CL07] Proposition 3.2].

Remark: Since $w \in K(S, 6)_{12}$ there exists $u \in K^*$ such that $(3u)^6w \in K(S, 12)$. Then an elliptic curve $E$ that Proposition 2.32 guarantees has the form

$$E : y^2 = x^3 - 3u^2j(j - 1728)x - 2u^3j(j - 1728)^2.$$  

The idea of Cremona–Lingham method is to consider all possible $w \in K(S, 6)_{12}$

\[\text{The set of } w \text{ is finite.}\]
and determine the possible $j \in \mathcal{O}_{K,S}$. For each $w$ they find $j$ by computing $S$–integral points on the Mordell curve $y^2 = x^3 - 1728w$.

**Proposition 2.33.** Let $K$ be a number field and $S$ a finite set of prime ideals of $K$. Let $w \in K(S, 6)$. Each $j \in \mathcal{O}_{K,S} \setminus \{0, 1728\}$ with $j^2 (j - 1728)^3 \equiv w \mod K^*6$ has the form $j = \frac{x^3}{w} = 1728 + \frac{y^2}{w}$, where $(x, y)$ is an $S$–integral point on the elliptic curve

$$E_w : y^2 = x^3 - 1728w$$

with $xy \neq 0$.

**Proof.** See [CL07, Proposition 3.3].

There are general algorithms with very good implementations of computing $S$–integral points for curves over $\mathbb{Q}$ ([Sma98], [ST94], [PZGH99], [Dev16]). If we forget the fact that the current implementations work only for curves over $\mathbb{Q}$, their big disadvantage is that they require a basis of the Mordell–Weil group. Finding a basis for the Mordell–Weil group is not an easy and finite problem yet. It is related to the BSD conjecture and the finiteness of $\text{III}(E/K)$ (see [Ste91] for a brief exposition of BSD from the computational point of view).

Since it is not always possible to find all $S$–integral points of the curves $E_w$, there are cases in practice where Cremona–Lingham method is not able to give us the complete set of curves $\mathcal{E}_{K,S}$. The new idea is to compute $j$ by computing the associate $\lambda$ using the relation of Theorem 2.5.
Chapter 3

Using $\lambda$–invariant

In this chapter we give a summary of the new method of computing $\mathcal{E}_{K,S}$. As we saw in the Cremona–Lingham method (see Section 2.7) given $K$ and $S$ it is enough to determine the $\overline{K}$–isomorphism classes of the curves in $\mathcal{E}_{K,S}$ in order to compute $\mathcal{E}_{K,S}$, equivalently to determine the $j$–invariants of the curves in $\mathcal{E}_{K,S}$. However, Cremona and Lingham determine $j$ by computing $S$–integral points on specific Mordell curves. But the only method of computing $S$–integral points on a curve which has existing implementation does require a Mordell–Weil basis.

The new idea is to compute the $j$–invariants by computing the $\lambda$–invariants of the curves. If we know $\lambda$ then by Theorem 2.5 we can compute $j$. However, $\lambda$ is not a random element, instead $\lambda$ satisfies special properties. For the rest of the chapter we assume that $E$ is an elliptic curve over $K$ with good reduction outside $S$, $j = j(E)$, $\lambda = \lambda(E)$ and $L = K(E[2])$ the 2–division field of $E$. We have to mention that the idea of using $\lambda$–invariant to compute $\mathcal{E}_{K,S}$ was suggested to John Cremona by Noam Elkies after a personal contact in July 2010.

Let $p$ be a prime not in $S^{(2)}$. We have mentioned in Section 2.1 that we
can find an integral model of $E$ that is minimal at $p$ with discriminant $\Delta$. Let $f_{2,E}$ be the 2–division polynomial of $E$ with roots $e_1$, $e_2$ and $e_3$. We define $g(x) = x^3 + b_2x^2 + 2^3b_4x + 2^4b_6$. An easy calculation shows that

$$2^4\Delta = \Delta(f_{2,E}) = 2^8 \prod_{1 \leq i < j \leq 3} (e_i - e_j)^2, \tag{3.1}$$

$$\Delta(g) = 2^t \Delta(f_{2,E}), \tag{3.2}$$

$$\Delta(g)^t = k^2 \Delta(L/K), \tag{3.3}$$

for some $k \in \mathcal{O}_K$ not equal to 0 and $t = 3$ if $[L : K] = 6$ and 1 otherwise.

We just showed that $p \nmid 2\Delta \Rightarrow p \nmid \Delta(L/K)$, thus the relative extension $L/K$ is unramified outside $S^{(2)}$. We know that $L/K$ is a Galois extension with Galois group isomorphic to a subgroup of $S_3$. So, we have proved the following.

**Proposition 3.1.** Let $E$ be an elliptic curve over a number field $K$ and good reduction outside a finite set $S$ of primes ideals of $K$. Then the 2–division field $L$ of $E$ is a Galois extension of $K$ unramified outside $S^{(2)}$ with Galois group isomorphic to a subgroup of $S_3$.

In addition, we have shown that $p \nmid 2\Delta \Rightarrow p \nmid (e_i - e_j)$ for $1 \leq i < j \leq 3$. Let $S_L = \{ \mathfrak{B} \subset \mathcal{O}_L : \mathfrak{B} \text{ is a prime such that } \exists p \in S^{(2)} \text{ with } \mathfrak{B}|p \}$ then by the definition of $\lambda$–invariant of $E$ we have that $\lambda \in \mathcal{O}_{L,S_L}^\ast$. By Theorem 2.5 $\mu := 1 - \lambda$ is also a $\lambda$–invariant of $E$ and satisfies the same properties as $\lambda$. So, $\mu \in \mathcal{O}_{L,S_L}^\ast$.

The new method has the following main steps:

- We compute all candidate 2–division fields for given $K$ and $S$. These are Galois extensions of $K$, unramified outside $S^{(2)}$ and $\text{Gal}(L/K) \simeq C_1, C_2,
$C_3$ or $S_3$. We use Kummer theory to find $L$ using the methods of Section 2.4.

- We solve the $S$–unit equation

$$\lambda + \mu = 1$$

where $\lambda, \mu \in \mathcal{O}_{L,S}^*$. We give necessary and sufficient conditions for $\lambda$ and $\mu$ which make the algorithms of solving $S$–unit equations effective (see Chapter 5).

- We compute $\mathcal{E}_{K,S}$ using Cremona–Lingham results as we described in section 2.7. We find the $j$–invariants of the curves using the $\lambda$–invariants we have computed in the previous step and the relation in Theorem 2.5.

In the rest of this thesis we go into the details of the main steps of the above method from both the algorithmic and theoretical point of view.

The most expensive part of the method is the solution of the $S$–unit equations. Since the rank of the groups involved in solving the $S$–unit equation have a significant effect on the running time of the algorithms to solve the equation, we will show that $\lambda$ and $\mu$ often lie in subgroups of smaller rank than $\mathcal{O}_{L,S}^*$, which improves the efficiency of the algorithm significantly. Moreover, we reduce the number of $S$–unit equations we have to solve making the assumption that we compute curves up to isogeny. This is a very natural assumption since the set $\mathcal{E}_{K,S}$ is a union of isogeny classes and computing isogenies is not computationally hard.
Chapter 4

Constructing 2–division fields

In this chapter we use Kummer theory, as it is described in Section 2.4, in order to develop a method that computes all candidate 2–division fields for the set of elliptic curves $\mathcal{E}_{K,S}$. The steps of the algorithm depend on the structure of the Galois group of the extension and the roots of unity that the base field $K$ contains. After presenting the algorithm in the next three section, we give a worked example in Section 4.4 and include pseudocode version of the algorithms in Section 4.5.

We assume that we are able to compute Selmer groups of number fields without any computational cost.

4.1 Quadratic extensions

Since $\zeta_2 = -1 \in K$ we can use Corollary 2.20. We compute all quadratic extensions of $K$ unramified outside $S$ using algorithm 1 page 44.
4.2 Cubic extensions

4.2.1 The case $\zeta_3 \in K$

The case $\zeta_3 \in K$ can be handled similarly to the quadratic case using Corollary 2.20 again. See algorithm 2 page 45.

4.2.2 The case $\zeta_3 \notin K$

In the case $\zeta_3 \notin K$ we have to use Theorem 2.24. We define $K_z = K(\zeta_3)$ and $S_z = \{\mathfrak{B} : \mathfrak{B} \text{ prime of } \mathcal{O}_{K_z}, \exists p \in S \text{ with } \mathfrak{B} | p\}$. We also denote $L_z = L(\zeta_3)$ and it holds $\text{Gal}(L_z/K) = C_6$. Since $\gcd([K_z : K], [L_z : K_z]) = 1$, a prime $p \in S$ is ramified in $L/K$ if and only if the primes in $S_z$ above $p$ are ramified in $L_z/K_z$.

We construct $L_z/K_z$ using the algorithm of the previous paragraph since $\zeta_3 \notin K_z$ now. That means $L_z = K_z(\sqrt[3]{a})$ with $a \in K_z(S_z, 3)$. However, it does not always hold that $\text{Gal}(L_z/K) = C_6$ for every element of $K_z(S_z, 3)$. By Theorem 2.24 $a$ should lie in $W_1$. By Proposition 2.25 that means

$$a \in W_1 \iff \frac{\tau(a)}{a^2} \in K_z^{*3} \iff \tau(a) a \in K_z^{*3} \iff N_{K_z/K}(a) \in K_z^{*3}.$$ 

Since $\zeta_3 \notin K$ we have that $K^* \cap K_z^{*3} = K_z^{*3}$. As a result we have $N_{K_z/K}(a) \in K_z^{*3} \iff N_{K_z/K}(a) \in K_z^{*3}$.

**Corollary 4.1.** With the above notation it holds that an element $a$ of $K_z(S_z, 3)$ lies in $W_1$ if and only if $N_{K_z/K}(a) \in K_z^{*3}$.

Let $a \tau(a) = \beta^3$ where $\beta \in K^*$. Since $\zeta_3 \notin K$ we understand that $\beta$ is unique.
We define $\tilde{\beta} = \frac{a}{\beta}$, then it holds
\[
\tilde{\beta}^{2 + \tau} = \tilde{\beta}^2 \tilde{\beta}^\tau = \frac{a^2}{\beta^2} \cdot \frac{\tau(a)}{\beta} = a.
\]

By the example at the end of Section 2.4 we can compute a defining polynomial of $L/K$ which is the following,
\[
f(X) = X^3 - 3eX - e \text{Tr}_{K_{\iota}/K}(\tilde{\beta}) = X^3 - 3\beta X - \text{Tr}_{K_{\iota}/K}(a),
\]
where $e = N_{K_{\iota}/K}(\tilde{\beta}) = \beta$ and $\text{Tr}_{K_{\iota}/K}(\tilde{\beta}) = \frac{\text{Tr}_{K_{\iota}/K}(a)}{\beta}$. See algorithm 3 page 45.

At the end we compute cubic extensions of $K$ unramified outside $S$ using the algorithm 4 page 46.

### 4.3 $S_3$ extensions

By the above sections we have a method of constructing all the quadratic and cubic Galois extensions of a number field $K$ which are unramified outside a finite set $S$ of prime ideals of $K$. For $S_3$ extensions of $K$ we use the fact that the group $S_3$ is solvable. This means that we are able to obtain an $S_3$ extension as a tower of a quadratic and cubic extensions. Even though we care about $S_3$ extensions in the rest of the section we describe an algorithm of constructing dihedral extensions $D_p$ with $p$ an odd prime $p \equiv 3 \mod 4$. For $p = 3$ it holds $D_3 = S_3$.

Let $K \subset M \subset L$ be a tower of Galois extensions where $\text{Gal}(M/K) \simeq C_2$ and\(^1\) $\text{Gal}(L/M) \simeq C_p$ where $p$ is an odd prime $p \equiv 3 \mod 4$. We fix the notation such that $\text{Gal}(L/M) = \langle \sigma \rangle$, $\text{Gal}(M/K) = \langle \tau \rangle$, $f(x) \in M[x]$ is a defining polynomial

\(^1\)See Chapter 2 for the details of constructing $C_p$ extensions.
of $L/M$ with the coefficient of $x^{p-1}$ equal to 0, $f^\tau = \tau(f)$ and $L^\tau$ is the splitting field of $f^\tau$. We use the same notation for any lift of $\tau$ and $\sigma$ to the absolute Galois group $\text{Gal}(\overline{K}/K)$.

**Proposition 4.2.** It holds that $L^\tau/M$ is a cyclic extension of order $p$.

*Proof.* Since $\tau(L) = L^\tau$ we have $[L^\tau : M] = p$ and it is Galois as the splitting field of a polynomial. \hfill \Box

**Theorem 4.3.** The extension $L/K$ is Galois if and only if $L = L^\tau$.

*Proof.* Let $\overline{K}$ be the algebraic closure of $K$. It holds that $L/K$ is Galois $\iff \forall \phi \in \text{Gal}(\overline{K}/K) : \phi(L) = L \iff \sigma(L) = L$ and $\tau(L) = L \iff \tau(L) = L$ since $L/M$ is Galois. \hfill \Box

From now on we assume that $L/K$ is Galois. The group $\text{Gal}(L/K)$ acts on the roots of $f$ as a subgroup of $S_p$. Since $p \equiv 3 \mod 4$ we know that $C_p$ is a subgroup of the alternating group $A_p$ but $D_p$ is not. The goal is to find an irreducible monic polynomial $h$ of degree $p$ over $K$ with splitting field $K(h)$ a subfield of $L$. Considering discriminants, we are able to check the case $\text{Gal}(K(h)/K) = C_p$ and as a result to distinguish:\[^2] $\text{Gal}(L/K) = D_p$ and $C_{2p}$.

For the special case $f = f^\tau$ (i.e. $f \in K[x]$) we have:

**Lemma 4.4.** Let $f$ be a defining polynomial of $L/M$ with $f \in K[x]$. Then $\Delta(f) \not= \Box$ in $K^*$ if and only if $\text{Gal}(L/K) \simeq D_p$.

*Proof.* Let $K(f)$ be the splitting field of $f$ over $K$. Since $L/K$ is Galois and $f$ is a defining polynomial of $L/M$ we have $K \subset K(f) \subset L$. From Proposition [2.15](#) we have that $\Delta(f) = \Box \iff \text{Gal}(K(f)/K) = C_p \iff \text{Gal}(L/K) = C_{2p}$. \hfill \Box

[^2] $D_p$ does not have a normal subgroup of order 2 while $C_{2p}$ has.
Now we assume that $f \neq f^\tau$. Write $f(x) = (x - a_1)(x - a_2) \cdots (x - a_p)$ and $f^\tau(x) = (x - b_1)(x - b_2) \cdots (x - b_p)$ with $a_i, b_j \in L$. We use $a_i, b_j$ to define a monic polynomial $h(x) \in K[x]$ whose splitting field is $L$.

In case Gal($L/K) = D_p$ we may assume that $\sigma$ permutes the roots $a_i$ and $b_j$ as $\sigma = (a_1 a_2 \cdots a_p)(b_1 b_2 \cdots b_p)$. Also we may assume that $\tau(a_1) = b_1$ and $\tau \sigma \tau = \sigma^{-1}$. Then by induction we conclude that $\tau(a_i) = b_{p+2-i}$ for $i = 2, \cdots, p$. We define $h$ to be,

$$h(x) = (x - a_1 - b_1)(x - a_2 - b_2) \cdots (x - a_p - b_p)$$

$$= (x - a_1 - \sigma(a_1))(x - a_2 - \sigma(a_2)) \cdots (x - a_p - \sigma(a_p))$$

with $a_1 + b_1 \neq 0$. By the choice of the action of $\tau$ and $\sigma$ on $a_i, b_j$ we can easily check that $\tau(h) = h$ and $\sigma(h) = h$, so $h \in K[x]$. We recall that we have assumed that the coefficient of $x^{p-1}$ of $f$ is equal to 0.

**Lemma 4.5.** Let $h$ and $f$ be as above then $h$ is irreducible in $K[x]$ and $K \subset K(h) \subset L$.

*Proof.* The fact that $K \subset K(h) \subset L$ comes from the definition of $h$ and the assumption that $L/K$ is Galois.

Let assume that $h$ is not irreducible in $K[x]$. Since $K \subset K(h) \subset L$, $[L : K] = 2p$ and the degree of $h$ is $p$ we conclude that $h$ has a root in $K$. Without loss of generality we assume $a_1 + b_1 = \delta \in K^*$. Applying $\sigma$ to $\delta$ we have $a_1 + b_1 = a_2 + b_2 = \cdots a_p + b_p = \delta$. Since the coefficient of $x^{p-1}$ in $f$ is equal to 0 we have that $a_1 + a_2 + \cdots + a_p = b_1 + b_2 + \cdots + b_p = 0$ which means $(a_1 + b_1) + (a_2 + b_2) + \cdots + (a_p + b_p) = 0$.

\[\text{If } a_1 + b_1 = 0 \text{ then } a_1 + b_2 \neq 0 \text{ since } b_1 \neq b_2. \text{ So we can change } h(x) \text{ with } h'(x) = (x - a_1 - \sigma(b_1))(x - a_2 - \sigma(b_2)) \cdots (x - a_p - \sigma(b_p)).\]
$0 \Rightarrow p\delta = 0 \Rightarrow \delta = 0$. So, we have $a_1 + b_1 = 0$, contradiction.

We summarize the previous results in the following theorem,

**Theorem 4.6.** Let $L/K$ be a Galois extension of degree $2p$ for $p \equiv 3 \mod 4$ and $M$ its quadratic subfield. Let $\tau \in \text{Gal}(L/K)$ be an element of order 2, $f \in M[x]$ a defining polynomial of $L/M$ such that the coefficient of $x^{p-1}$ is zero, $f^\tau = \tau(f)$ and $h$ as in (4.1). Then we have,

(i) If $f = f^\tau$ then $\Delta(f) \neq \square$ in $K^*$ if and only if $\text{Gal}(L/K) \simeq D_p$.

(ii) If $f \neq f^\tau$ then $h \in K[x]$ and irreducible over $K$. Moreover, $\Delta(h) \neq \square$ in $K^*$ if and only if $\text{Gal}(L/K) \simeq D_p$.

Since the $p$–Selmer group of any number field with respect to any finite set of primes $S$ is a finite abelian group, we can deduce now the following,

**Theorem 4.7.** Let $K$ be a number field, $S$ a finite set of prime of $K$. Then the number of Galois extensions $L/K$ unramified outside $S$ with Galois group equal to $C_2$, $C_3$ or $S_3$ is finite.

We summarize the above analysis of computing Galois $S_3$ extensions of $K$ unramified outside $S$ in the algorithm 5 page 46.

### 4.4 Example

Here we consider the case $K = \mathbb{Q}$ and $S = \{2, 3, 23\}$. We understand that $\mathcal{O}_{K,S}^* = \langle -1, 2, 3, 23 \rangle$ and we can easily compute the 15 quadratic extensions of $\mathbb{Q}$ unramified outside $S$. These are the fields $\mathbb{Q}(\sqrt{d})$ where $d \in \{-1, \pm 2, \pm 3, \pm 23, \pm 6, \pm 46, \pm 69, \pm 138\}$. 41
Since $\zeta_3 \not\in \mathbb{Q}$ we have to consider the case where we adjoin $\zeta_3$ in order to find the cubic extensions of $\mathbb{Q}$ unramified outside $S$. Following the relevant algorithm we find only one cubic extension with defining polynomial $x^3 - 3x - 1$ and discriminant $3^4$.

The algorithm for the $S_3$ extensions computes 37 fields. We represent each field with a cubic polynomial over $\mathbb{Q}$ whose splitting field is an $S_3$ extension.

<table>
<thead>
<tr>
<th>field $x^3 - ax - b$</th>
<th>discriminant $-2^m3^n23^r$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$x^3 - 138x - 644$</td>
<td>$-2^63^823^4$</td>
</tr>
<tr>
<td>$x^3 - x^2 + 8x - 6$</td>
<td>$-2^63^8$</td>
</tr>
<tr>
<td>$x^3 - 3x - 4$</td>
<td>$-2^63^8$</td>
</tr>
<tr>
<td>$x^3 + 69x - 230$</td>
<td>$-2^63^823^4$</td>
</tr>
<tr>
<td>$x^3 - x - 1$</td>
<td>$-23^3$</td>
</tr>
<tr>
<td>$x^3 - 23$</td>
<td>$-3^723^4$</td>
</tr>
<tr>
<td>$x^3 - 2$</td>
<td>$-2^43^7$</td>
</tr>
<tr>
<td>$x^3 - x^2 - 61x - 167$</td>
<td>$-2^43^323^4$</td>
</tr>
<tr>
<td>$x^3 - 92$</td>
<td>$-2^43^723^4$</td>
</tr>
<tr>
<td>$x^3 - 3$</td>
<td>$-3^{11}$</td>
</tr>
<tr>
<td>$x^3 - 207$</td>
<td>$-3^{11}23^4$</td>
</tr>
<tr>
<td>$x^3 - 69$</td>
<td>$-3^{11}23^4$</td>
</tr>
<tr>
<td>$x^3 - 18x - 30$</td>
<td>$-2^43^{11}$</td>
</tr>
<tr>
<td>$x^3 - 414$</td>
<td>$-2^43^{11}23^4$</td>
</tr>
<tr>
<td>$x^3 - 276$</td>
<td>$-2^43^{11}23^4$</td>
</tr>
<tr>
<td>$x^3 - 6$</td>
<td>$-2^43^{11}$</td>
</tr>
<tr>
<td>$x^3 - 828$</td>
<td>$-2^43^{11}23^4$</td>
</tr>
<tr>
<td>$x^3 - 138$</td>
<td>$-2^{43}1123^4$</td>
</tr>
<tr>
<td>-------------------</td>
<td>------------------</td>
</tr>
<tr>
<td>$x^3 - 18x - 6$</td>
<td>$2^{43}1123^3$</td>
</tr>
<tr>
<td>$x^3 - 6x - 3$</td>
<td>$3^723^3$</td>
</tr>
<tr>
<td>$x^3 - 54x - 150$</td>
<td>$2^{43}1123^3$</td>
</tr>
<tr>
<td>$x^3 - 36x - 78$</td>
<td>$2^{43}1123^3$</td>
</tr>
<tr>
<td>$x^3 - 6x - 20$</td>
<td>$-2^63723^3$</td>
</tr>
<tr>
<td>$x^3 + 69x - 46$</td>
<td>$-2^93823^4$</td>
</tr>
<tr>
<td>$x^3 - 3x - 10$</td>
<td>$-2^93^8$</td>
</tr>
<tr>
<td>$x^3 - x^2 - 15x - 29$</td>
<td>$-2^923^4$</td>
</tr>
<tr>
<td>$x^3 + 69x - 874$</td>
<td>$-2^93823^4$</td>
</tr>
<tr>
<td>$x^3 - 93x - 346$</td>
<td>$-2^93823^3$</td>
</tr>
<tr>
<td>$x^3 - 9x - 6$</td>
<td>$2^93^11$</td>
</tr>
<tr>
<td>$x^3 - x^2 + 8x + 40$</td>
<td>$-2^93^323^4$</td>
</tr>
<tr>
<td>$x^3 + 3x - 2$</td>
<td>$-2^93^7$</td>
</tr>
<tr>
<td>$x^3 + 69x - 322$</td>
<td>$-2^93723^4$</td>
</tr>
<tr>
<td>$x^3 + 69x - 138$</td>
<td>$-2^93723^4$</td>
</tr>
<tr>
<td>$x^3 - 9x - 42$</td>
<td>$-2^931123^3$</td>
</tr>
<tr>
<td>$x^3 - 18x - 40$</td>
<td>$-2^93723^3$</td>
</tr>
<tr>
<td>$x^3 + 63x - 66$</td>
<td>$-2^931123^3$</td>
</tr>
<tr>
<td>$x^3 - 81x - 306$</td>
<td>$-2^931123^3$</td>
</tr>
</tbody>
</table>

These are the same fields as in the database of number fields by John Jones and David Roberts ([JR14]).
4.5 Algorithms

Here we present the steps of computing all Galois extensions $L$ of $K$ with $\text{Gal}(L/K) \subset S_3$ and unramified outside $S$ in algorithmic form.

**Algorithm 1 Quadratic extensions unramified outside $S$**

1: procedure QUADRATIC($K, S$)
2: Calculate $K(S, 2)$.
3: Fields = $\emptyset$.
4: for $a \in K(S, 2)$ and $a \neq 1$ do
5: Evaluate $L = K(\sqrt{a})$.
6: Calculate the relative discriminant $\Delta(L/K)$.
7: if $\exists p \notin S$ s.t. $p | \Delta(L/K)$ then
8: $L$ is not a solution.
9: else
10: Add $L$ in Fields.
11: end if
12: end for
13: return Fields.
14: end procedure
### Algorithm 2 Cubic extensions unramified outside $S$ and $\zeta_3 \in K$

1: **procedure** CUBICINCLUDE_ZETA($K, S$)  
2: \> Calculate $K(S, 3)$.  
3: \> Fields = $\emptyset$.  
4: \> for $a \in K(S, 3)$ and $a \neq 1$ do  
5: \> \> Evaluate $L = K(\sqrt[3]{a})$.  
6: \> \> Calculate the relative discriminant $\Delta(L/K)$.  
7: \> \> if $\exists p \notin S$ s.t. $p \mid \Delta(L/K)$ then  
8: \> \> \> $L$ is not a solution.  
9: \> \> else  
10: \> \> \> Add $L$ in Fields.  
11: \> end if  
12: end for  
13: **return** Fields.  
14: **end procedure**

### Algorithm 3 Cubic extensions unramified outside $S$ and $\zeta_3 \notin K$

1: **procedure** CUBICNOTINCLUDE_ZETA($K, S$)  
2: \> Construct $K_z = K(\zeta_3)$.  
3: \> Calculate $S_z = \{ \mathfrak{B} : \mathfrak{B}$ is a prime of $O_{K_z}, \exists p \in S$ with $\mathfrak{B} \mid p \}$.  
4: \> Calculate $K_z(S_z, 3)$.  
5: \> Fields = $\emptyset$.  
6: \> for $a \in \ker \left( K_z(S_z, 3) \xrightarrow{\text{Norm}} K(S, 3) \right)$ and $a \neq 1$ do  
7: \> \> Find $\beta \in K^*$ s.t. $\beta^3 = N_{K_z/K}(a)$.  
8: \> \> Define $L = K(\theta)$, where $\theta$ is a root of $f(X) = X^3 - 3\beta X - Tr_{K_z/K}(a)$.  
9: \> \> Calculate the relative discriminant $\Delta(L/K)$.  
10: \> \> if $\exists p \notin S$ s.t. $p \mid \Delta(L/K)$ then  
11: \> \> \> $L$ is not a solution.  
12: \> \> else  
13: \> \> \> Add $L$ in Fields.  
14: \> end if  
15: end for  
16: **return** Fields.  
17: **end procedure**
Algorithm 4 Cubic extensions unramified outside $S$

```plaintext
procedure CUBIC($K, S$)
    if $\zeta_3 \in K$ then
        return CUBIC_INCLUDE_ZETA($K, S$)
    else
        return CUBIC_NOT_INCLUDE_ZETA($K, S$)
    end if
end procedure
```

Algorithm 5 $S_3$ extensions unramified outside $S$

```plaintext
1: procedure $S_3$_EXTENSIONS($K, S$)
2:   Fields = $\emptyset$.
3:   for $M$ in QUADRATIC($K, S$) do
4:     Evaluate $S_M = \{\mathfrak{B} : \mathfrak{B}$ prime of $\mathcal{O}_M, \exists p \in S$ with $\mathfrak{B} | p\}$. 
5:     for $L$ in CUBIC($M, S_M$) do
6:       Let $f = x^3 - ax + b$ be a defining polynomial of $L/M$.
7:       if $f = f^\tau$ then
8:         Evaluate $\Delta(f)$.
9:         if $\Delta(f) \not\in K^{*2}$ then
10:            Add $L$ in Fields.
11:       end if
12:     else
13:       Let $r_1$ be a root of $f$ and $r_2$ a root of $f^\tau$.
14:       $r = r_1 + r_2$.
15:       if $r = 0$ then
16:          Replace $r_2$ with another root of $f^\tau$.
17:       end if
18:       Let $h$ be the minimal polynomial of $r$ over $K$.
19:       Evaluate $\Delta(h)$.
20:       if $\Delta(h) \not\in K^{*2}$ then
21:          Add $L$ in Fields.
22:     end if
23:   end if
24: end for
25: end for
26: return Fields.
27: end procedure
```
Chapter 5

Solving $S$–unit equations

In this chapter we show that the solutions $\lambda$ and $\mu$ of an $S$–unit equation associate to an elliptic curve $E \in \mathcal{E}_{K,S}$ lie in subgroups of the full $S$–unit group with smaller rank than the full $S$–unit group. Moreover, we show how we can reduce the number of the $S$–equations we have to solve.

5.1 Algorithms for solving $S$–unit equations

In this section we have a short exposition of the main steps of the existing general algorithmic method for solving an $S$–unit equation. Most of the techniques and details can be found in the work of De Weger, Tzanakis, Smart and Wildanger ([Weg88], [Weg87], [TdW89], [TW92], [Sma95], [Sma98], [Sma99], [Wil00], [Wil97], [EG16]).

The main idea of solving the $S$–unit equation (2.7) over a number field $K$ is the following. Let $\langle g_{0,1}, g_{1,1}, \ldots, g_{n,1} \rangle$ and $\langle g_{0,2}, g_{1,2}, \ldots, g_{m,2} \rangle$ be sets of generators for $G_1$ and $G_2$ respectively, where $g_{0,1}, g_{0,2}$ are the generators of the torsion parts.
and $g_{i,1}, g_{j,2}$ for $i = 1, \cdots, n$ and $j = 1, \cdots, m$ are bases of the free parts of $G_1$ and $G_2$. Then we know that

$$x = \prod_{i=0}^{n} g_{i,1}^{a_i}$$

$$y = \prod_{j=0}^{m} g_{j,2}^{b_j}$$

where $a_i, b_j \in \mathbb{Z}$. We define $\Xi = \max_{i,j}(|a_i|, |b_j|)$. The goal is to find a small upper bound $\Xi_0$ of $\Xi$ that can be used for practical computations. After computing $\Xi_0$ we make use of a sieve argument in order to reduce the number of cases we have to check. To sum up, the three main steps are the following.

- Using results by Baker’s theory of linear forms of logarithms we find an upper bound $\Xi_0$ for $\Xi$.

- Using lattice approximation reduction methods we reduce the upper bound $\Xi_0$ to a number that can be used for practical computations. For this step we have to deal with $p$–adic analysis, $p$–adic logarithms, the LLL–algorithm, approximation lattices and the shortest vector problem.

- We apply a sieve in order to find the solutions.

It is important to mention that the rank of $G_1$ and $G_2$ are crucial for the last two steps. The main goal of the rest of the chapter is to reduce the rank of the group where $\lambda$ and $\mu$ lie and the number of the $S$–unit equations we have to solve.

## 5.2 Reduce the number of $S$–unit equations

Since solving an $S$–unit equation is the most expensive part of the method it is really worthwhile to reduce the number of equations we have to solve. By a result
of Ribet and Mazur ([Rib76, Proposition 2.1]) we have,

**Proposition 5.1.** Let $E$ be an elliptic curve with full two torsion. Then $E$ is isogenous to a curve without full two torsion.

Let $E_1/K$ be an elliptic curve with one rational point of order 2. We assume that $E_1$ is of the form,

$$E_1 : y^2 = x(x^2 + ax + b)$$

with $b, a^2 - 4b \neq 0$. We have seen in Section 2.1 that $E_1$ is isogenous to the elliptic curve

$$E_2 : Y^2 = X(X^2 - 2aX + a^2 - 4b).$$

An easy calculation shows that $\Delta(E_1) = 2^{4b^2}(a^2 - 4b)$ and $\Delta(E_2) = 2^{8b}(a^2 - 4b)^2$.

Let $L_1$ and $L_2$ be the 2–division fields of $E_1$ and $E_2$, respectively. By the definition of the 2–division field and the discriminant of an elliptic curve we have that $\Delta(L_i/K) \equiv \Delta(E_i) \mod K^*2$ for $i = 1, 2$.

**Proposition 5.2.** Let $E_1, E_2$ be as above. If $(\overline{K})$ is the Hilbert symbol relative to $K$ then it holds,

$$\left( \frac{\Delta(E_1), \Delta(E_2)}{K} \right) = 1.$$

**Proof.** The equation $\Delta(E_1) x^2 + \Delta(E_2) y^2 = z^2$ has the non–trivial solution $(\frac{1}{4b}, \frac{1}{8(a^2 - 4b)}, a)$. \qed

In case $E_1$ has full 2–torsion the following proposition holds.

**Proposition 5.3.** Let $E_1$ be as above such that $x(x^2 + ax + b)$ splits completely
in $K$. If $E_2, E_3, E_4$ are the three 2–isogenous to $E_1$ curves then
\[ \prod_{i=2}^{4} \Delta(E_i) \equiv -1 \mod K^*, \] \[ \left( \frac{\Delta(E_i), \Delta(E_j)}{K} \right) = 1 \]
for $2 \leq i < j \leq 4$.

**Proof.** Let assume that $x(x^2 + ax + b) = x(x - e_1)(x - e_2)$ where $e_1, e_2 \in K^*$. As we have shown earlier $\Delta(E_2) = 2^8b(a^2 - 4b)^2 \equiv b = e_1e_2 \mod K^*$. Using a change of variables in $E_1$ we can show that $\Delta(E_3) \equiv e_1(e_1 - e_2) \mod K^*$ and $\Delta(E_4) \equiv e_2(e_2 - e_1) \mod K^*$. Now multiplying everything together we have the first relation.

By symmetry we prove the second relation only for the pair $E_2$ and $E_3$. We can see that the equation $\Delta(E_2)x^2 + \Delta(E_3)y^2 = z^2$ has the non–trivial solution $(w_2^{-1}, w_3^{-1}, e_1)$ where $\Delta(E_2) = e_1e_2w_2^2$ and $\Delta(E_3) = e_1(e_1 - e_2)w_3^2$, for some $w_2, w_3 \in K^*$.

Since computing Hilbert symbols in $K$ and 2–isogenous curves can been done very quickly in practice, the last two propositions allows us to reduce the number of $S$–unit equations we have to solve when the 2–division field is a trivial or a quadratic extension of $K$ by computing isogenous curves.

Moreover, when the initial set $S$ does not contain a prime $p$ above 2 the following proposition also decreases the number of candidate 2–division fields.

**Proposition 5.4.** Let $E$ be an elliptic curve over $K$ with good reduction outside $S$ and $L/K$ its 2–division field. Let $p$ be a prime of $K$ above 2 not in $S$. Then $^1 \text{ord}_p(\Delta(L/K)) \equiv 0 \mod 2$.

\[ ^1 \text{In case } [L : K] = 6 \text{ we can prove that } \text{ord}_p(\Delta(L/K)) \equiv 0 \mod 2 \iff \text{ord}_p(\Delta(L_6/K)) \equiv 0 \mod 2 \text{ where } L_6 \text{ is the cubic subfield of } L/K. \]
Proof. Let $\Delta$ be the discriminant of $E$ and $f_{2,E}$ its $2$–division polynomial. By Proposition 2.31 we have that $\text{ord}_p(\Delta) \equiv 0 \mod 2$. By equations (3.1)–(3.3) we obtain $(2^8\Delta)^t = k^2\Delta(L/K)$ for some $k \in K^*$. Thus, $\text{ord}_p(\Delta(L/K)) \equiv 0 \mod 2$. 

5.3 Reducing the rank

We recall that $K$ is a number field, $S$ is a finite set of prime ideals of $K$, $E$ is an elliptic curve over $K$ with good reduction outside $S$, $\lambda$ is a $\lambda$–invariant of $E$, $\mu = 1 - \lambda$, $L$ is the $2$–division field of $E$ and $S_L = \{ B \subset \mathcal{O}_L : B$ is a prime such that $\exists p \in S^{(2)}$ with $B|p \}. The pair $(\lambda, \mu)$ is a solution of the $S$–unit equation

$$\lambda + \mu = 1$$

(5.1)

where both $\lambda, \mu \in \mathcal{O}_{L,S_L}^*$. For the rest of the chapter we also assume that the $j$–invariant of $E$ is not equal to 0 and 1728.

The group $\text{PGL}_2(\mathbb{Z})$ acts on $K$ with the usual way,

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot z = \frac{az + b}{cz + d}$$

where $z \in K$ and $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \text{PGL}_2(\mathbb{Z})$.

Since we have assumed that $j \neq 0, 1728$, by the relation of part (iii) of Theorem

51
we see that all the elements of $\Lambda$ are distinct. We define

$$T = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad R = \begin{pmatrix} 0 & 1 \\ -1 & 1 \end{pmatrix} \in \text{PGL}_2(\mathbb{Z})$$

where $T$ and $R$ have order 2 and 3 respectively. Let $G := \langle T, S \rangle \simeq S_3$ then $G$ acts on $\Lambda$ as a permutation group on the roots of the polynomial $F_j(x) = \prod_{\lambda' \in \Lambda} (x - \lambda') = (x^2 - x + 1)^3 - \frac{j}{28} x^2 (1 - x)^2 \in K[x]$. Because $L \supseteq K(\lambda)$ the splitting field of $F_j$ is a subfield of $L$. From the above we understand that $\text{Gal}(L/K)$ acts on $\Lambda$ in the same way as a subgroup of $G$.

We divide into cases, according to the structure of $\text{Gal}(L/K)$. We recall that

$$j = 2^8 \frac{(\lambda^2 - \lambda + 1)^3}{\lambda^2 (1 - \lambda)^2}$$

$$w = j^2 (j - 1728)^3,$$

$$O^*_{L,K,S_L,1} = \{x \in O^*_{L,S_L} : \text{Norm}_{L/K}(x) = 1\},$$

$$O^*_{L,K,S_L,\pm 1} = \{x \in O^*_{L,S_L} : \text{Norm}_{L/K}(x) = \pm 1\}.$$

### 5.3.1 $\text{Gal}(L/K)$ is trivial

In the case $\text{Gal}(L/K)$ is the trivial group the elliptic curve $E$ has full 2–torsion and $\lambda, \mu \in K^*$. We have to solve the $S$–unit equation \([5.1]\) for $\lambda, \mu \in O_{K,S(2)}$ or make use of Proposition \([5.1]\).

### 5.3.2 $\text{Gal}(L/K) \simeq C_2$

In this case the following theorem holds,
Theorem 5.5. Suppose that $\Lambda \subset \mathcal{O}_{L,S_L}$ is associated with an elliptic curve defined over $K$. Then there exists $\lambda \in \Lambda$ such that $\lambda \in \mathcal{O}_{L,K,S_L,1}^*$. Conversely, let $\lambda \in \mathcal{O}_{L,S_L}^*$ and $j, w, \mu$ as usual. If $\mu \in \mathcal{O}_{L,S_L}^*$ and $\lambda \in \mathcal{O}_{L,K,S_L,1}^*$ then $j \in \mathcal{O}_{K,S}$. Moreover, if $w \in K(S, 6)_{12}$ then $j$ is the $j$–invariant of an elliptic curve with good reduction outside $S^{(6)}$.

Proof. Let $\tau$ be a generator of $\text{Gal}(L/K)$ then from the compatibility of the action of $G$ and $\text{Gal}(L/K)$ on the set $\Lambda$ we can choose $\lambda \in \Lambda$ such that $\tau(\lambda) = T \cdot \lambda = \frac{1}{\lambda}$. As a result,

$$\text{Norm}_{L/K}(\lambda) = 1.$$  

Conversely, if $\text{Norm}_{L/K}(\lambda) = 1$ that means $\tau(\lambda) = \frac{1}{\lambda}$ and then $\tau(j) = j$. Since, $\lambda, \mu \in \mathcal{O}_{L,S_L}^*$ we have that $v_B(\lambda^2 - \lambda + 1) \geq 0$ for all $B \not\in S_L$ and then $j \in \mathcal{O}_{K,S}$. Moreover, if $w \in K(S, 6)_{12}$ then by Proposition 2.32 there exists an elliptic curve over $K$ with $j$–invariant equal to $j$ and good reduction outside $S^{(6)}$.  

Remark: It is important to mention that $\mu$ does not satisfy extra conditions apart from the fact that $\mu \in \mathcal{O}_{L,S_L}^*$.

5.3.3 $\text{Gal}(L/K) \simeq C_3$

In this case the following theorem holds,

Theorem 5.6. Let $\text{Gal}(L/K) = \langle \sigma \rangle$. Suppose that $\Lambda \subset \mathcal{O}_{L,S_L}^*$ is associated with an elliptic curve defined over $K$. Then there exists $\lambda \in \Lambda$ satisfying the following conditions,

(i) $\lambda \in \mathcal{O}_{L,K,S_L,\pm 1}^*$.
(ii) \( \sigma(\lambda) = \frac{1}{\mu} \).

Conversely, let \( \lambda \in \mathcal{O}_{L,S_L}^* \) and \( j, w, \mu \) as usual. If \( \mu \in \mathcal{O}_{L,S_L}^* \) and (i)–(ii) hold then \( j \in \mathcal{O}_{K,S} \). Moreover, if \( w \in K(S,6)_{12} \) then \( j \) is the \( j \)-invariant of an elliptic curve with good reduction outside \( S^{(6)} \).

**Proof.** As in the quadratic case we can assume that \( \sigma(\lambda) = S \cdot \lambda = \frac{1}{1-\lambda} = \frac{1}{\mu} \). Then an immediate calculation shows that \( \text{Norm}_{L/K}(-\lambda) = 1 \). The proof of the converse is similar to Theorem 5.5. \( \square \)

**Remark:** From the condition \( \sigma(\lambda) = \frac{1}{\mu} \) we also see that \( \text{Norm}_{L/K}(-\mu) = 1 \). Actually, one can prove that we can replace condition (ii) with the condition \( \mu \in \mathcal{O}_{L,K,S,L}^* \).

### 5.3.4 \( \text{Gal}(L/K) \cong S_3 \)

Finally, for the case \( \text{Gal}(L/K) \cong S_3 \) we have a similar result,

**Theorem 5.7.** Let \( \text{Gal}(L/K) \cong S_3 = \langle \sigma, \tau \rangle \) such that \( \sigma^3 = \tau^2 = 1 \) and \( \tau \sigma \tau = \sigma^{-1} \). Suppose that \( \Lambda \subset \mathcal{O}_{L,S_L}^* \) is associated with an elliptic curve defined over \( K \).

Then, there exists \( \lambda \in \Lambda \) satisfying the following conditions,

(i) \( \lambda \in \mathcal{O}_{L,L^\ast,S_L,1}^* \),

(ii) \( \lambda \in \mathcal{O}_{L,L^\ast,S_L,\pm 1}^* \),

(iii) \( \sigma(\lambda) = \frac{1}{\mu} \).

Conversely, let \( \lambda \in \mathcal{O}_{L,S_L}^* \) and \( j, w, \mu \) as usual. If \( \mu \in \mathcal{O}_{L,S_L}^* \) and (i)–(iii) hold then \( j \in \mathcal{O}_{K,S} \). Moreover, if \( w \in K(S,6)_{12} \) then \( j \) is the \( j \)-invariant of an elliptic curve with good reduction outside \( S^{(6)} \).
Proof. As in the proofs of Theorems 5.5 and 5.6 we can assume that $\sigma(\lambda) = S \cdot \lambda = \frac{1}{1-\lambda}$ and $\tau(\lambda) = T \cdot \lambda = \frac{1}{\lambda}$. The last two equations show that $\text{Norm}_{L/L^*}(-\lambda) = 1$ and $\text{Norm}_{L/L^*}(\lambda) = 1$. The proof of the converse is similar to Theorem 5.5. \qed

Theorems 5.5, 5.6 and 5.7 show that the solutions of an $S$–unit equation associated to an elliptic curve with good reduction outside $S$ lie in subgroups of the full $S$–unit group with smaller rank. According to Theorems 5.5, 5.6 and 5.7 we define $G_\lambda$ and $G_\mu$ subgroups of $O^*_{L,S}$ as follow.

**Definition 5.8.** Let $K, S, E, L, S_L, \lambda$ and $\mu$ as usual. We define

- $G_\lambda = G_\mu = O_{K,S}^{(2)}$ if $[L : K] = 1$,

- $G_\lambda = O_{L,K,S_L,1}^*$ and $G_\mu = O_{L,S_L}^*$ if $[L : K] = 2$,

- $G_\lambda = O_{L,K,S_L,\pm 1}^*$ and $G_\mu = \sigma(G_\lambda)$ if $[L : K] = 3$ where $\text{Gal}(L/K) = \langle \sigma \rangle$,

- $G_\lambda = O_{L,L^*,S_L,1}^* \cap O_{L,L^*,S_L,\pm 1}^*$ and $G_\mu = \sigma(G_\lambda)$ where $\text{Gal}(L/K) \simeq S_3 = \langle \sigma, \tau \rangle$ such that $\sigma^3 = \tau^2 = 1$ and $\tau \sigma \tau = \sigma^{-1}$.

In practice Theorems 5.5, 5.6 and 5.7 allow us to solve $S$–unit equations effectively since both the reduction and sieve steps are computational easier. In the next chapter we modify Wildanger’s and Smart’s ideas in such a way that we obtain a sieve step suitable to our problem. The symmetries we have for $\lambda$ and $\mu$ in the $C_3$ and $S_3$ cases play an important role in the sieve.

\footnote{We recall that in this case $G_\lambda = G_\mu$.}
5.4 Example

We continue the example in Section 4.4 where $K = \mathbb{Q}$ and $S = \{2, 3, 23\}$. Using Propositions 5.1, 5.2 and 5.3, we can reduce the number of $S$–unit equations we have to solve over quadratic extensions since we compute curves up to isogeny.

By Proposition 5.1, we understand that we only need to compute curves with only one non–trivial point of order 2. We split these curves in two categories; (i) those which are isogenous to a curve without full 2–torsion and (ii) the curves which are isogenous to a curve with full 2–torsion.

For the first set of curves we deduce that we have to solve $S$–unit equations only for the fields $\mathbb{Q}(\sqrt{d})$ where $d \in \{2, 3, 6, \pm 23, 46, 69, 138\}$ in order to compute curves up to isogeny. For example, for $d \neq 1$ we have that $\left(\frac{-2d}{q}\right) = 1$ only for $d = 2, 3, 6$. By Proposition 5.2 we have that an elliptic curve $E_d$ with quadratic 2–division field but without full 2–torsion and isogenous to a curve $E_{-2}$ with 2–division field $\mathbb{Q}(\sqrt{-2})$ can only have 2–division field $\mathbb{Q}(\sqrt{d})$ for $d = 2, 3, 6$. That means we can skip the direct computation of elliptic curves with 2–division field $\mathbb{Q}(\sqrt{-2})$ if we have already computed all the curves with 2–division field $\mathbb{Q}(\sqrt{d})$ for $d = 2, 3, 6$ by computing isogenous curves. Continue the above procedure for all possible pairs we end up with the smaller set $\{2, 3, 6, \pm 23, 46, 69, 138\}$.

However, they may exist curves in the second set but they do not have 2–division field any of the fields of the form $\mathbb{Q}(\sqrt{d})$ for $d \in \{2, 3, 6, \pm 23, 46, 69, 138\}$. We apply Proposition 5.3 for all possible triples $\{(d_1, d_2, d_3)\}$ with $d_1, d_2, d_3 \in \{\pm 1, -2, -3, -6, -46, -69, -138\}$ and the only triple that we have is $(1, 1, -1)$.

So, we deduce that we have to solve $S$–unit equations only for the fields $\mathbb{Q}(\sqrt{d})$
where \( d \in \{-1, 2, 3, 6, \pm 23, 46, 69, 138\} \) in order to compute curves up to isogeny with at least one rational point of order 2. In the following table we show the rank of \( G_\lambda \) and \( \mathcal{O}_{L,S_L}^* \) according to Theorem 5.5. We recall that in this case \( G_\mu = \mathcal{O}_{L,S_L}^* \).

<table>
<thead>
<tr>
<th>field</th>
<th>rank((G_\lambda))</th>
<th>rank((\mathcal{O}_{L,S_L}^*))</th>
</tr>
</thead>
<tbody>
<tr>
<td>( t^2 + 1 )</td>
<td>0</td>
<td>3</td>
</tr>
<tr>
<td>( t^2 - 2 )</td>
<td>2</td>
<td>5</td>
</tr>
<tr>
<td>( t^2 - 3 )</td>
<td>2</td>
<td>5</td>
</tr>
<tr>
<td>( t^2 - 6 )</td>
<td>2</td>
<td>5</td>
</tr>
<tr>
<td>( t^2 + 23 )</td>
<td>2</td>
<td>5</td>
</tr>
<tr>
<td>( t^2 - 46 )</td>
<td>2</td>
<td>5</td>
</tr>
<tr>
<td>( t^2 - 23 )</td>
<td>1</td>
<td>4</td>
</tr>
<tr>
<td>( t^2 - 69 )</td>
<td>1</td>
<td>4</td>
</tr>
<tr>
<td>( t^2 - 138 )</td>
<td>1</td>
<td>4</td>
</tr>
</tbody>
</table>

In Section 4.4 we saw that there is only one cubic extension over \( \mathbb{Q} \) unramified outside \( S \) which is the splitting field of \( x^3 - 3x - 1 \). Using Theorem 5.6 one shows that rank\((G_\lambda)\) = 2 while rank\((\mathcal{O}_{L,S_L}^*)\) = 5. We also recall that in this case \( G_\lambda = G_\mu \).

Finally in Section 4.4 we have 37 Galois extensions of \( \mathbb{Q} \) unramified outside \( S \) such that Gal\((L/\mathbb{Q})\) = \( S_3 \). Using Theorem 5.7 we have the following table for the rank of \( G_\lambda \) and \( \mathcal{O}_{L,S_L}^* \). Again we recall that in this case rank\((G_\lambda)\) = rank\((G_\mu)\) but \( G_\lambda \neq G_\mu \).
<table>
<thead>
<tr>
<th>field</th>
<th>rank($G_\lambda$)</th>
<th>rank($O^*_{L,S_L}$)</th>
</tr>
</thead>
<tbody>
<tr>
<td>$x^3 - 138x - 644$</td>
<td>2</td>
<td>7</td>
</tr>
<tr>
<td>$x^3 - x^2 + 8x - 6$</td>
<td>3</td>
<td>9</td>
</tr>
<tr>
<td>$x^3 - 3x - 4$</td>
<td>3</td>
<td>9</td>
</tr>
<tr>
<td>$x^3 + 69x - 230$</td>
<td>2</td>
<td>7</td>
</tr>
<tr>
<td>$x^3 - x - 1$</td>
<td>2</td>
<td>9</td>
</tr>
<tr>
<td>$x^3 - 23$</td>
<td>2</td>
<td>7</td>
</tr>
<tr>
<td>$x^3 - 2$</td>
<td>2</td>
<td>7</td>
</tr>
<tr>
<td>$x^3 - x^2 - 61x - 167$</td>
<td>2</td>
<td>7</td>
</tr>
<tr>
<td>$x^3 - 92$</td>
<td>1</td>
<td>5</td>
</tr>
<tr>
<td>$x^3 - 3$</td>
<td>3</td>
<td>9</td>
</tr>
<tr>
<td>$x^3 - 207$</td>
<td>2</td>
<td>7</td>
</tr>
<tr>
<td>$x^3 - 69$</td>
<td>2</td>
<td>7</td>
</tr>
<tr>
<td>$x^3 - 18x - 30$</td>
<td>2</td>
<td>7</td>
</tr>
<tr>
<td>$x^3 - 414$</td>
<td>1</td>
<td>5</td>
</tr>
<tr>
<td>$x^3 - 276$</td>
<td>1</td>
<td>5</td>
</tr>
<tr>
<td>$x^3 - 6$</td>
<td>2</td>
<td>7</td>
</tr>
<tr>
<td>$x^3 - 828$</td>
<td>1</td>
<td>5</td>
</tr>
<tr>
<td>$x^3 - 138$</td>
<td>1</td>
<td>5</td>
</tr>
<tr>
<td>$x^3 - 18x - 6$</td>
<td>3</td>
<td>10</td>
</tr>
<tr>
<td>$x^3 - 6x - 3$</td>
<td>4</td>
<td>12</td>
</tr>
<tr>
<td>$x^3 - 54x - 150$</td>
<td>3</td>
<td>10</td>
</tr>
<tr>
<td>$x^3 - 36x - 78$</td>
<td>3</td>
<td>10</td>
</tr>
<tr>
<td>Expression</td>
<td>Value 1</td>
<td>Value 2</td>
</tr>
<tr>
<td>-----------------------------------</td>
<td>---------</td>
<td>---------</td>
</tr>
<tr>
<td>$x^3 - 6x - 20$</td>
<td>3</td>
<td>9</td>
</tr>
<tr>
<td>$x^3 + 69x - 46$</td>
<td>2</td>
<td>8</td>
</tr>
<tr>
<td>$x^3 - 3x - 10$</td>
<td>3</td>
<td>10</td>
</tr>
<tr>
<td>$x^3 - x^2 - 15x - 29$</td>
<td>2</td>
<td>8</td>
</tr>
<tr>
<td>$x^3 + 69x - 874$</td>
<td>2</td>
<td>8</td>
</tr>
<tr>
<td>$x^3 - 93x - 346$</td>
<td>3</td>
<td>9</td>
</tr>
<tr>
<td>$x^3 - 9x - 6$</td>
<td>3</td>
<td>11</td>
</tr>
<tr>
<td>$x^3 - x^2 + 8x + 40$</td>
<td>3</td>
<td>9</td>
</tr>
<tr>
<td>$x^3 + 3x - 2$</td>
<td>3</td>
<td>9</td>
</tr>
<tr>
<td>$x^3 + 69x - 322$</td>
<td>2</td>
<td>7</td>
</tr>
<tr>
<td>$x^3 + 69x - 138$</td>
<td>2</td>
<td>7</td>
</tr>
<tr>
<td>$x^3 - 9x - 42$</td>
<td>3</td>
<td>9</td>
</tr>
<tr>
<td>$x^3 - 18x - 40$</td>
<td>3</td>
<td>9</td>
</tr>
<tr>
<td>$x^3 + 63x - 66$</td>
<td>3</td>
<td>9</td>
</tr>
<tr>
<td>$x^3 - 81x - 306$</td>
<td>3</td>
<td>9</td>
</tr>
</tbody>
</table>
Chapter 6

Efficient Sieve

In Chapter 5 we briefly explained the main steps of the general algorithmic method of solving an $S$–unit equation (2.7). We also recall them here. Let $\langle g_{0,1}, g_{1,1}, \ldots, g_{n,1} \rangle$ and $\langle g_{0,2}, g_{1,2}, \ldots, g_{m,2} \rangle$ be sets of generators for $G_1$ and $G_2$ respectively, where $g_{0,1}, g_{0,2}$ are the generators of the torsion parts and $g_{i,1}, g_{j,2}$ for $i = 1, \ldots, n$ and $j = 1, \ldots, m$ are bases of the free parts of $G_1$ and $G_2$. Then we know that

$$x = \prod_{i=0}^{n} g_{i,1}^{a_i} \quad \quad y = \prod_{j=0}^{m} g_{j,2}^{b_j}$$

where $a_i, b_j \in \mathbb{Z}$. We define $\Xi = \max_{i,j} (|a_i|, |b_j|)$. The goal is to find a small upper bound $\Xi_0$ of $\Xi$ that can be used for practical computations. After computing $\Xi_0$ we make use of a sieve argument in order to reduce the number of cases we have to check. To sum up, the three main steps are the following.

- Using results by Baker’s theory of linear forms of logarithms we find a upper bound $\Xi_0$ for $\Xi$. 

60
• Using lattice approximation reduction methods we reduce the upper bound \( \Xi_0 \) to a number that can be used for practical computations. For this step we have to deal with \( p \)-adic analysis, \( p \)-adic logarithms, LLL–algorithm, approximation lattices and the problem of the shortest vector.

• We apply a sieve in order to find the solutions.

In the current chapter we study the final sieve step of the special case (5.1) of (2.7) where now \( x, y \) are called \( \lambda, \mu \) and are related to the \( \lambda \)-invariants of the set \( \mathcal{E}_{K,S} \). General sieve methods have been suggested by Smart and Wildanger ([Sma99], [Wil00], [Wil97], [EG16]). However, we modify Smart’s and Wildanger’s ideas in such a way that we benefit from Theorems 5.5, 5.6 and 5.7 and the symmetries they introduce in the solutions.

Since we have proved that \( \lambda \) and \( \mu \) may lie in different subgroups of \( \mathcal{O}_{L,S}^* \), we denote by \( G_\lambda \) and \( G_\mu \) the subgroups of \( \mathcal{O}_{L,S}^* \) where \( \lambda \) and \( \mu \) lie according to the Definition 5.8. Let \( G_\lambda = \langle \lambda_0, \lambda_1, \ldots, \lambda_n \rangle \) and \( G_\mu = \langle \mu_0, \mu_1, \ldots, \mu_m \rangle \) be sets of generators where \( \lambda_0 \) and \( \mu_0 \) are generators of the torsion part and \( \lambda_i, \mu_j \) are bases for the free parts. For the rest of the chapter we fix bases for \( G_\lambda \) and \( G_\mu \) and we express \( \lambda \) and \( \mu \) as a multiplicative combination of the bases,

\[
\lambda = \prod_{i=0}^{n} \lambda_i^{x_i} \quad \mu = \prod_{j=0}^{m} \mu_j^{y_j}.
\]

In the \( C_3 \) and \( S_3 \) cases where \( \sigma(\lambda) = \frac{1}{\mu} \) we can make a choice of bases for \( G_\lambda \) and \( G_\mu \) such that \( \lambda \) and \( \mu \) have the same vector exponents, i.e. \( n = m \) and \( x_i = y_i \) for \( i = 0, \ldots, n \). Moreover, by Theorem 5.6 we have that \( G_\lambda = G_\mu \) in the \( C_3 \) case and by Theorem 5.7 we have that \( G_\mu = \sigma(G_\lambda) \) in the \( S_3 \) case. It is also important
to mention that in practice and for the analysis that follows it seems to be better to choose bases for $G_\lambda$ and $G_\mu$ such that some of the generators of the bases lie in $\mathcal{O}_K^*$. Let $M_L$ be the set of places of $L$ then we define,

$$S_\lambda = \{ \mathfrak{B} \in M_L : |x|_\mathfrak{B} \neq 1 \text{ for some } x \in G_\lambda \}$$  \hspace{1cm} (6.1)$$

$$S_\mu = \{ \mathfrak{B} \in M_L : |x|_\mathfrak{B} \neq 1 \text{ for some } x \in G_\mu \}$$  \hspace{1cm} (6.2)$$

An important observation from Theorems 5.5, 5.6 and 5.7 is that when $G_\lambda, G_\mu \neq \mathcal{O}_L, S_L$, then $S_\lambda, S_\mu$ do not contain prime ideals $\mathfrak{B}$ which are above non split primes of $K$. This holds because $G_\lambda, G_\mu$ are intersections of kernels of suitable norm maps.

The idea of the sieve is to split the set of candidate solutions into two sets in each step. The first set contains solutions with low exponents and small absolute values at all places in $S_\lambda$ and $S_\mu$ and the second set contains the solutions with high absolute value at one or more places in $S_\lambda$ or $S_\mu$. Then we repeat this procedure until we find all the solutions.

The sieve starts assuming that we have two vectors $B_0 = \left( b_0^{(0)}, b_1^{(0)}, \ldots, b_n^{(0)} \right)$ and $C_0 = \left( c_0^{(0)}, c_1^{(0)}, \ldots, c_m^{(0)} \right)$ such that for every pair $(\lambda, \mu)$, $|x_i| \leq b_i^{(0)}$ and $|y_j| \leq c_j^{(0)}$ for all $i = 0, \ldots, n$ and $j = 0, \ldots, m$.

\footnote{Both finite and infinite places.}
For a fixed subset $I$ of $\{0, 1, \cdots, n\}$ we define

$$S_I = \{ \mathfrak{B} \in S_\lambda : \exists i \in I \text{ such that } |\lambda_i|_\mathfrak{B} \neq 1 \}$$

$$\lambda_I = \prod_{i \in I} \lambda_i^{x_i}.$$ 

We denote by $I^\infty = \{ i \in \{0, 1, \cdots, n\} : \lambda_i \in O_K^* \}$, $S_\lambda^\infty = S_I^\infty$ and $\lambda^\infty := \lambda_I^\infty$.

Similarly, we define $S_J$ for a fixed subset $J$ of $\{0, 1, \cdots, m\}$, $\mu_J$, $J^\infty$, $S_\mu^\infty$ and $\mu^\infty$.

### 6.1 Trivial solutions for $|x - 1|_p \ll 1$

Let $G = \langle g_0, g_1, \cdots, g_n \rangle$ be a finitely generated subgroup of $K^*$ for a number field $K$ where $g_0$ is a generator of the torsion part and $g_i$, for $i = 1, \cdots, n$, are a basis of the free part of $G$. In the sieve we want to be able to show when an inequality of the form

$$|g - 1|_p \leq \delta \ll 1$$

with $g \in G$, $p$ a place of $K$ and $\delta \in (0, 1)$ has only trivial solutions.

Let $g = g_0^{x_0} \prod_{i=1}^n g_i^{x_i}$ with $x_0 \in \mathbb{Z}$ and $|x_i| \leq b_i$ where $b_i$ are positive integers for $i = 1, \cdots, n$. A trivial solution of (6.3) is an element $g \in G$ such that $x_i = 0$ for $i = 1, \cdots, n$. According to the type of $p$ we consider two cases.
6.1.1 Infinite place

For a complex number \( z \in \mathbb{C} \) with \( |z - 1| \leq \delta < 1 \) we have that \( |\log |z|| \leq \log(\frac{1}{1-\delta}) \). Then for \( |g - 1|_p \leq \delta \) it holds,

\[
|\log |g|_p| \leq \delta' = \begin{cases} 
\log(\frac{1}{1-\delta}) & \text{p is real}, \\
\frac{1}{2} \log(\frac{1}{1-\sqrt{\delta}}) & \text{p is complex}.
\end{cases}
\]

Since \( \delta \) is small then \( \delta' \) is small too. We choose an integer constant \( C \) of the size \( 10^n \) and we create the lattice \( \mathcal{L} \) generated by the columns of the matrix\(^2\)

\[
A = \begin{pmatrix}
1 & 0 \\
& \ddots \\
0 & 1 & 0 \\
[C \log |g_1|_p] & \cdots & [C \log |g_{n-1}|_p] & [C \log |g_n|_p]
\end{pmatrix} \in \mathbb{Z}^{n \times n},
\]

where \([\cdot]\) denotes the nearest integer function. Using the LLL–algorithm (see Chapter 2) we are able to find a lower bound \( \ell_b \) for \( \ell(\mathcal{L}, \vec{0}) \). Following the approach in [Sma99, Lemma 3] we have the following lemma.

**Lemma 6.1.** Let

\[
Q = \sum_{i=1}^{n-1} b_i^2 + \left( \sum_{i=1}^{n} b_i + C \delta' \right)^2
\]

If \( \ell_b^2 > Q \), then there does not exist a non–trivial solution of (6.3).

**Proof.** Let

\[
\Phi = \sum_{i=1}^{n} x_i[C \log |g_i|_p].
\]

\(^2\)We assume that \( |g_n|_p \neq 1 \).
Then
\[ |\Phi - C \left( \sum_{i=1}^{n} x_i \log |g_i|_p \right) | \leq \frac{\sum_{i=1}^{n} b_i}{2}. \]

Thus
\[ |\Phi| \leq |\Phi - C \log |g|_p| + |C \log |g|_p| \leq \frac{\sum_{i=1}^{n} b_i}{2} + C\delta'. \]

Let consider the lattice point \( \vec{z} = A\vec{x} \), where \( \vec{x} = (x_1, x_2, \cdots, x_n)^t \). Then \( \vec{z} = (x_1, \cdots, x_{n-1}, \Phi) \). If \( \vec{z} \neq \vec{0} \), we must have
\[ \ell_b^2 \leq \ell(\mathcal{L}, \vec{0})^2 \leq \sum_{i=1}^{n-1} b_i^2 + \Phi^2 \leq Q. \]

If \( \vec{z} = \vec{0} \) then \( x_i = 0 \) for all \( i = 1, \cdots, n \).

The choice of \( C \) in the above lemma is not fixed and we have to increase it if the criterion of the lemma is not satisfied. The only difference between Lemma 6.1 and Lemma 3 in [Sma99] is that we allow the exponent of each generator to have different upper bound. This small difference ends up to be very useful in practice as we will see later.

### 6.1.2 Finite place

Let \( p \) be a prime ideal of the number field \( K \). Let \( p \) be the rational prime below \( p \) and \( e_p \) and \( f_p \) the ramification and residual degree of \( p \). We assume that
\[ \delta' = \frac{-\log \delta}{e_p f_p \log p} \geq 1 \]
which is not a very restricted condition since \( \delta \) is very small in practice.

In the following lines we will show the \( p \)-adic analogue of Lemma [6.1]. Since
\[ |g - 1|_p \leq \delta < 1 \] we have that \( \text{ord}_p(g) = 0 \). By Lemma 2.16 we can find a finite set of elements \( h_0, h_1, h_2, \ldots, h_t \in K^* \) such that

\[
g = h_0 \prod_{i=1}^{t} h_i^{y_i}
\]

where \( \text{ord}_p(h_i) = 0 \) for \( i = 0, \ldots, t \) and \( |y_i| \leq |x_i| \leq b_i \) for \( i = 1, \ldots, t \).

Then we set

\[
\Theta := \log_p(g) = \log_p(h_0) + \sum_{i=1}^{t} y_i \log_p(h_i) \in K_p.
\]

Since \( \delta' \geq 1 \) and Section 2.3

\[
\text{ord}_p(\Theta) = \text{ord}_p(\log_p(g)) = \text{ord}_p(g - 1) \geq -\frac{\log \delta}{e_p f_p \log p} = \delta'.
\]

Let \( d = e_p f_p = [K_p : \mathbb{Q}_p] \) and \( K_p = \mathbb{Q}_p(\phi) \). Then we have

\[
\Theta = \sum_{i=0}^{d-1} \Theta_i \phi^i.
\]

where \( \Theta_i = \nu_0,i + \sum_{j=1}^{t} y_j \nu_j,i \) with \( \nu_j,i \in \mathbb{Q}_p \) for \( i = 0, \ldots, d - 1 \). As in [TW92, page 257] we can show that

\[
\text{ord}_p(\Theta_i) \geq \delta' - \frac{\text{ord}_p(D(\phi))}{2} =: c_1
\]

where \( D(\phi) = \text{disc}_{K_p/\mathbb{Q}_p}(1, \phi, \ldots, \phi^{d-1}) \). We choose \( \xi \in \mathbb{Q}_p \) such that

\[
\text{ord}_p(\xi) = \min_{0 \leq j \leq t} \left( \min_{0 \leq i \leq d-1} (\text{ord}_p(\nu_j,i)) \right) =: c_2
\]

66
Dividing $\Theta_i$ by $\xi$ we get

$$\frac{\Theta_i}{\xi} = \kappa_{0,i} + \sum_{j=1}^{t} y_j \kappa_{j,i}$$

for $i = 0, \ldots, d - 1$ and so $\kappa_{j,i} \in \mathbb{Z}_p$. We have that

$$\text{ord}_p\left(\frac{\Theta_i}{\xi}\right) \geq c_1 - c_2 =: c_3$$

Since $c_1 = \delta' - \frac{\text{ord}_p(D(\phi))}{2}$ and $\delta'$ is big in practice we assume that $c_3 \geq 1$. We choose $u \in \mathbb{N}$ such that $u \leq c_3$. For $a \in \mathbb{Z}_p$ we denote by $a^{[u]}$ the positive integer less than $p^u$ such that $a \equiv a^{[u]} \mod p^u$. We define the lattice $\mathcal{L}$ by the columns of the matrix

$$A = \begin{pmatrix}
1 & 0 \\
\vdots & \ddots \\
0 & 1 & \kappa_{[u]}^{[u]} & \kappa_{[u]}^{[u]} & p^u & 0 \\
\vdots & \vdots & \ddots & \ddots & \ddots & \ddots \\
\kappa_{[u]}^{[u]} & \kappa_{[u]}^{[u]} & p^u & \ldots & \ldots & \ldots \\
\kappa_{[u]}^{[u]} & \kappa_{[u]}^{[u]} & p^u & \ldots & \ldots & \ldots
\end{pmatrix} \in \mathbb{Z}^{(t+d) \times (t+d)}.$$

Furthermore, we define the vector $\vec{y} = (0, \ldots, 0, -\kappa_{0,0}^{[u]}, \ldots, -\kappa_{0,d-1}^{[u]})^t \in \mathbb{Z}^{t+d}$. Again using LLL–algorithm we can find a lower bound $\ell_b$ for $\ell(\mathcal{L}, \vec{y})$. Following the approach in [Sma99, Lemma 4] we have the following lemma.

**Lemma 6.2.** If $\ell_b^2 > \sum_{i=1}^{t} b_i^2$ then there does not exist a non–trivial solution of (6.3).
Proof. Since \( \text{ord}_p(\frac{\Theta}{\xi}) \geq c_3 \geq u \) we have that

\[
z_i = \frac{\kappa^{[u]}_{0,i} + \sum_{j=1}^{t} y_j \kappa^{[u]}_{j,i}}{p^u} \in \mathbb{Z}
\]

for \( i = 0, \cdots, d - 1 \). We consider the lattice point \( \vec{z} = A\vec{h} \) where \( \vec{h} = (y_1, \cdots, y_t, -z_1, \cdots, -z_{d-1})^t \in \mathbb{Z}^{t+d} \). Because

\[
\vec{z} - \vec{y} = (y_1, \cdots, y_t, 0, \cdots, 0)^t,
\]

we understand that either \( \ell^2_b \leq \ell(\mathcal{L}, \vec{y}) \leq \sum_{i=1}^{t} b_i^2 \) or \( \vec{z} = \vec{y} \). Since we have the assumption \( \ell^2_b > \sum_{i=1}^{t} b_i^2 \) we get that \( y_i = 0 \) for \( i = 1, \cdots, t \). \( \square \)

6.2 Decomposing the solutions

In this section we show how we can decompose the pairs \((\lambda, \mu)\) of solutions of (5.1) in sets which we can either show they have only trivial solutions, or we can find the solutions they contain. Again, we have cases according to the structure of \( \text{Gal}(L/K) \).

There are two immediate observations for a pair of solutions \((\lambda, \mu)\) that we use without mentioning them further. Let \( \mathfrak{B} \) be a prime ideal of \( L \). Then,

- \( \text{ord}_\mathfrak{B}(\lambda) > 0 \Rightarrow \text{ord}_\mathfrak{B}(\mu) = 0 \) and by symmetry \( \text{ord}_\mathfrak{B}(\mu) > 0 \Rightarrow \text{ord}_\mathfrak{B}(\lambda) = 0 \).
- \( \text{ord}_\mathfrak{B}(\lambda) < 0 \Leftrightarrow \text{ord}_\mathfrak{B}(\mu) < 0 \) and then it holds \( \text{ord}_\mathfrak{B}(\lambda) = \text{ord}_\mathfrak{B}(\mu) \).
6.2.1 Quadratic extensions

Let $\tau$ be the generator of $\text{Gal}(L/K)$. By Theorem 5.5 we can assume that we are looking for pairs of solutions $(\lambda, \mu)$ such that $\tau(\lambda) = \frac{1}{\lambda}$. Moreover, we have mentioned earlier that $S_\lambda$ contains prime ideals $\mathfrak{B}$ above split primes of $K$ and by Definition 5.8 we recall that $G_\mu = \mathcal{O}^*_L,S_\lambda$. In addition $\text{ord}_\mathfrak{B}(\lambda) = -\text{ord}_{\tau(\lambda)}(\lambda)$ for all $\lambda \in G_\lambda$. For one of the conjugate prime ideals $\mathfrak{B} \in S_\lambda$ we prove that there do not exist pairs $(\lambda, \mu)$ such that $|\text{ord}_\mathfrak{B}(\lambda)|$ is ‘large’. We do this by showing that,

$$|\mu - 1|_{\mathfrak{B}} \leq \delta \ll 1$$

has no non–trivial solutions using Lemma 6.2 for a suitable choice of $\delta$. We do the same for $\mathfrak{B} \in S_\mu$ and $\lambda$ instead of $\mu$ in order to prove that there do not exist pairs $(\lambda, \mu)$ such that $|\text{ord}_\mathfrak{B}(\mu)|$ is ‘large’. We use the new upper bounds on $|\text{ord}_\mathfrak{B}(\lambda)|$ and $|\text{ord}_\mathfrak{B}(\mu)|$ for the prime ideals of $S_\lambda$ and $S_\mu$ respectively to get new vectors $B_1 = (b_0^{(1)}, b_1^{(1)}, \ldots, b_n^{(1)})$ and $C_1 = (c_0^{(1)}, c_1^{(1)}, \ldots, c_m^{(1)})$ such that $|x_i| \leq b_i^{(1)}$ and $|y_j| \leq c_j^{(1)}$ for $i = 0, 1, \ldots, n$ and $j = 0, 1, \ldots, m$.

Since we have chosen only finite places $\mathfrak{B} \in S_\lambda$ we have not yet reduced $b_i^{(1)}$ and $c_j^{(1)}$ for the unit generators. The way we reduce the bounds for the unit generators is to split the set of solutions in two sets, where the first set contains solutions with smaller exponents, and try to show that the second set contains no solutions. We observe that $\mathfrak{B} \in S_\lambda^\infty \iff \tau(\mathfrak{B}) \in S_\lambda^\infty$.

**Definition 6.3.** Let $B = (b_0, b_1, \ldots, b_n) \in \mathbb{N}^{n+1}$ and $C = (c_0, c_1, \ldots, c_m) \in \mathbb{N}^{m+1}$. Then for $R > 1$ we define,

$$\mathcal{L}^2_\infty(B,C,R) = \{(\lambda, \mu) : |x_i| \leq b_i, |y_j| \leq c_j, \log |\lambda|_{\mathfrak{B}} \leq \log R, \forall \mathfrak{B} \in S_\lambda^\infty\}$$

69
Let
\[ R_{1,\infty} = \max_{\mathcal{B} \in S_{\infty}^\lambda} \exp \left( \sum_{i=0}^{n} b_i^{(1)} |\log |\lambda_i|_{\mathcal{B}}| \right). \]

**Lemma 6.4.** Every pair \((\lambda, \mu)\) of solutions lies in \(L^2_\infty(B_1, C_1, R_{1,\infty}).\)

**Proof.** For a \(\mathcal{B} \in S_{\infty}^\lambda\) we have,
\[
|\log |\lambda_i|_{\mathcal{B}}| \leq \sum_{i=0}^{n} |x_i||\log |\lambda_i|_{\mathcal{B}}| \leq \sum_{i=0}^{n} b_i^{(1)} |\log |\lambda_i|_{\mathcal{B}}|
\leq \max_{\mathcal{B} \in S_{\infty}^\lambda} \left( \sum_{i=0}^{n} b_i^{(1)} |\log |\lambda_i|_{\mathcal{B}}| \right) = \log(R_{1,\infty}).
\]

\[\square\]

**Definition 6.5.** Let \(B = (b_0, b_1, \cdots, b_n) \in \mathbb{N}^{n+1}\) and \(C = (c_0, c_1, \cdots, c_m) \in \mathbb{N}^{m+1}\). For \(\mathcal{B} \in S_{\infty}^\lambda\) and \(1 < R' < R\) we define,
\[
\mathcal{T}_B^2(B, C, R, R') = \left\{ (\lambda, \mu) \in L^2_\infty(B, C, R) : |\mu - 1|_{\mathcal{B}} < \frac{1}{R'} \right\}.
\]

We need the following lemma.

**Lemma 6.6.** There exists a computable constant \(c_{1,\infty} > 0\) such that
\[
|x_i| \leq c_{1,\infty} \max_{\mathcal{B} \in S_{\infty}^\lambda} (|\log |\lambda_{\infty}|_{\mathcal{B}}|),
\]
for all \(i \in I_{\infty}^\lambda\).

**Proof.** We can assume that \(I_{\infty}^\lambda = \{1, 2, \cdots, t\}\) and \(S_{\infty}^\lambda = \{\mathcal{B}_1, \mathcal{B}_2, \cdots, \mathcal{B}_u\}\) with
\( t \leq u \). We define the matrix

\[
M = \begin{pmatrix}
\log |\lambda_1|_{B_1} & \cdots & \log |\lambda_t|_{B_1} \\
\vdots & \ddots & \vdots \\
\log |\lambda_1|_{B_u} & \cdots & \log |\lambda_t|_{B_u}
\end{pmatrix}
\]

By the choice of \( I^\infty \) and \( S^\infty_\lambda \) there exists a \( t \times t \) submatrix of \( M \) which is invertible. Among all these submatrices we choose one, which we call \( M_s \), whose inverse has the maximal infinity norm. We define \( c_{1,\infty} = \|M_s^{-1}\| \). Then we can deduce that

\[
|x_i| \leq c_{1,\infty} \max_{B \in S^\infty_\lambda} (|\log |\lambda_\infty|_B|) \quad \text{for all} \quad i \in I^\infty.
\]

Now we have all the necessary ingredients to show how we split \( L^2_\infty(B, C, R) \).

**Proposition 6.7.** Let \( 1 < R_{k+1} < R_k \), \( B_k = \left( b_0^{(k)}, b_1^{(k)}, \ldots, b_n^{(k)} \right) \in \mathbb{N}^{n+1} \) and \( C_k = \left( c_0^{(k)}, c_1^{(k)}, \ldots, c_m^{(k)} \right) \in \mathbb{N}^{m+1} \). Then we have,

\[
L^2_\infty(B_k, C_k, R_k) = L^2_\infty(B_{k+1}, C_{k+1}, R_{k+1}) \cup \bigcup_{B \in S^\infty_\lambda} T^2(B_k, C_k, R_k, R_{k+1})
\]

where \( C_{k+1} = C_k \), \( b_i^{(k+1)} = \min \left( b_i^{(k)}, c_{1,\infty} \cdot (\log R_{k+1} + c_{2,\infty}) \right) \) for \( i \in I^\infty \), otherwise \( b_i^{(k+1)} = b_i^{(k)} \), and \( c_{2,\infty} = \max_{B \in S^\infty_\lambda} \left( \sum_{i \notin I^\infty} b_i^{(k)} |\log |\lambda_i|_B| \right) \).

**Proof.** Let \( (\lambda, \mu) \in L^2_\infty(B_k, C_k, R_k) \) but \( (\lambda, \mu) \notin L^2_\infty(B_k, C_k, R_{k+1}) \). That means there exists \( B \in S^\infty_\lambda \) such that \( |\lambda|_B > R_{k+1} \) or \( |\lambda|_B < \frac{1}{R_{k+1}} \). In the first case we have that,

\[
|\lambda|_B > R_{k+1} \iff |\tau(\lambda)|_{\tau(B)} > R_{k+1} \iff |\lambda - 1|_{\tau(B)} < \frac{1}{R_{k+1}}.
\]

\[
71
\]
In the second case we have

$$|\lambda|_B < \frac{1}{R_{k+1}} \iff |\mu - 1|_B < \frac{1}{R_{k+1}}.$$

We have shown that

$$(\lambda, \mu) \notin \mathcal{L}_\infty^2(B_k, C_k, R_{k+1}) \Rightarrow \bigcup_{B \in S_\infty} T^2(B_k, C_k, R_k, R_{k+1})$$

Now for $(\lambda, \mu) \in \mathcal{L}_\infty^2(B_k, C_k, R_{k+1})$ we have that

$$|\log |\lambda\infty|_B| \leq |\log |\lambda|_B| + |\log \frac{\lambda}{\lambda\infty}|_B| < \log R_{k+1} + c_{2,\infty}.$$ 

By Lemma 6.6 we deduce that

$$|x_i| \leq c_{1,\infty} \cdot (\log R_{k+1} + c_{2,\infty})$$

for all $i \in I^\infty$. Thus $(\lambda, \mu) \in \mathcal{L}_\infty^2(B_{k+1}, C_{k+1}, R_{k+1})$. 

Proposition 6.7 is very useful in practice because proving that the sets $T^2(B_k, C_k, R_k, R_{k+1})$ do not contain non-trivial solutions can be done quickly as we showed in the previous section. Moreover, the constants $c_{1,\infty}$ and $c_{2,\infty}$ can be easily computed in practice and since we have small $|\text{ord}_B(\lambda)|$ for $B \notin S_\infty$, $c_{2,\infty}$ is small.
6.2.2 Cubic extensions

Let $\sigma$ be a generator of $\text{Gal}(L/K)$. By Theorem 5.6 we can assume that we are looking for pairs of solutions $(\lambda, \mu)$ such that $\sigma(\lambda) = \frac{1}{\mu}$. Moreover, we have made a choice of $G_\lambda$ and $G_\mu$ such that $\lambda$ and $\mu$ have the same vector exponents, i.e. $n = m$ and $x_i = y_i$ for $i = 0, 1, \cdots, n$. This can be done by taking $\mu_i = \sigma(\frac{1}{\lambda_i})$.

So, we have to consider only the bound vector for $\lambda$ in each step of the sieve and we observe that $I^\infty = J^\infty$. We recall that $G_\lambda = G_\mu$ and as a result $S_\lambda = S_\mu$ and $S_\lambda^\infty = S_\mu^\infty$.

As we mentioned earlier $S_\lambda$ and $S_\mu$ contain only prime ideals $\mathfrak{B}$ above split primes of $K$. For each one of the conjugate prime ideals $\mathfrak{B} \in S_\lambda$ we prove that there do not exist pairs $(\lambda, \mu)$ such that $|\text{ord}_\mathfrak{B}(\lambda)|$ is ‘large’. We do this by showing that, $|\mu - 1|_\mathfrak{B} \leq \delta \ll 1$

has no non–trivial solutions using Lemma 6.2 for a suitable choice of $\delta$. We use the new upper bounds on $|\text{ord}_\mathfrak{B}(\lambda)|$ for all prime ideals of $S_\lambda$ to get a new vector $B_1 = (b_0^{(1)}, b_1^{(1)}, \cdots, b_n^{(1)})$ such that $|x_i| \leq b_i^{(1)}$ for $i = 0, 1, \cdots, n$.

**Definition 6.8.** Let $B = (b_0, b_1, \cdots, b_n) \in \mathbb{N}^{n+1}$. Then for $R > 1$ we define, $L^3_\infty(B, R) = \{(\lambda, \mu) : |x_i| \leq b_i, |\log |\lambda||_\mathfrak{B} \leq \log R, \forall \mathfrak{B} \in S_\lambda^\infty \}$

Let $R_{1,\infty}$ be as above, then

**Lemma 6.9.** Every pair $(\lambda, \mu)$ of solutions lies in $L^3_\infty(B_1, R_{1,\infty})$.

**Proof.** The proof is similar to Lemma 6.4.
Definition 6.10. Let $B = (b_0, b_1, \cdots, b_n) \in \mathbb{N}^{n+1}$. For $\mathcal{B} \in S_{\infty}^{\lambda}$ and $1 < R' < R$ we define,

$$T^3_{\mathcal{B}}(B, R, R') = \left\{ (\lambda, \mu) \in \mathcal{L}_{\infty}^3(B, R) : \begin{array}{l}
|\mu - 1|_{\mathcal{B}} < \frac{1}{R'} \text{ or } \\
|\lambda - 1|_{\sigma(\mathcal{B})} < \frac{1}{R'}
\end{array} \right\}.$$ 

Let $c_{1,\infty}$ be as in Lemma 6.6.

Proposition 6.11. Let $1 < R_{k+1} < R_k$, $B_k = \left( b_{0}^{(k)}, b_{1}^{(k)}, \cdots, b_{n}^{(k)} \right) \in \mathbb{N}^{n+1}$. Then we have,

$$\mathcal{L}_{\infty}^3(B_k, R_k) = \mathcal{L}_{\infty}^3(B_{k+1}, R_{k+1}) \cup \bigcup_{\mathcal{B} \in S_{\infty}^{\lambda}} T^3_{\mathcal{B}}(B_k, R_k, R_{k+1}).$$

where $b_i^{(k+1)} = \min\left( b_i^{(k)}, c_{1,\infty} \cdot (\log R_k + c_{2,\infty}) \right)$ for $i \in I_{\infty}$, otherwise $b_i^{(k+1)} = b_i^{(k)}$, and $c_{2,\infty} = \max_{\mathcal{B} \in S_{\infty}^{\lambda}} \left( \sum_{i \notin I_{\infty}} b_i^{(k)} \log |\lambda_i|_{\mathcal{B}} \right)$.

Proof. The proof is similar to Proposition 6.7.

6.2.3 $S_3$ extensions

Let $\sigma$ and $\tau$ be the generator of $\text{Gal}(L/K)$ such that $\sigma^3 = \tau^2 = 1$ and $\tau \sigma \tau = \sigma^{-1}$. By Theorem 5.7 we can assume that we are looking for pairs of solutions $(\lambda, \mu)$ such that $\tau(\lambda) = \frac{1}{\lambda}$ and $\sigma(\lambda) = \frac{1}{\mu}$. Moreover, we have made a choice of $G_{\lambda}$ and $G_{\mu}$ such that $\lambda$ and $\mu$ have the same vector exponents i.e. $n = m$ and $x_i = y_i$ for $i = 0, 1, \cdots, n$. This can be done by taking $\mu_i = \sigma\left( \frac{1}{\lambda_i} \right)$ and so it is enough to consider only the bound vector for $\lambda$. So we understand that $G_{\mu} = \sigma(G_{\lambda})$ and $I_{\infty} = J_{\infty}$.
As we mentioned earlier, $S_{\lambda}$ and $S_{\mu}$ contain only prime ideals $\mathfrak{B}$ above split primes of $K$. Again, the first step is to find an upper bound of $|\text{ord}_{\mathfrak{B}}(\lambda)|$ for each prime ideal $\mathfrak{B} \in S_{\lambda}$ by proving that,

$$|\mu - 1|_{\mathfrak{B}} \leq \delta \ll 1$$

has no non-trivial solutions using Lemma 6.2 for a suitable choice of $\delta$. We use the new upper bounds on $|\text{ord}_{\mathfrak{B}}(\lambda)|$ for all prime ideals of $S_{\lambda}$ to get a new vector

$$B_1 = \left( b_0^{(1)}, b_1^{(1)}, \ldots, b_n^{(1)} \right)$$

such that $|x_i| \leq b_i^{(1)}$ for $i = 0, 1, \ldots, n$.

**Definition 6.12.** Let $B = (b_0, b_1, \ldots, b_n) \in \mathbb{N}^{n+1}$. Then for $R > 1$ we define,

$$\mathcal{L}_{\infty}^6(B, R) = \left\{ (\lambda, \mu) : x_i \leq b_i, \quad \frac{|\log |\lambda|_{\mathfrak{B}}|}{\log R} \leq \log R, \forall \mathfrak{B} \in S_{\infty}^{\lambda} \cup S_{\infty}^{\mu} \right\}.$$ 

Let $R_{1,\infty}$ be as above, then

**Lemma 6.13.** Every pair $(\lambda, \mu)$ of solutions lies in $\mathcal{L}_{\infty}^6(B_1, R_{1,\infty})$.

**Proof.** The proof is similar to Lemma 6.4. \hfill \Box

**Definition 6.14.** Let $B = (b_0, b_1, \ldots, b_n) \in \mathbb{N}^{n+1}$. For $\mathfrak{B} \in S_{\infty}^{\lambda} \cup S_{\infty}^{\mu}$ and $1 < R' < R$ we define,

$$\mathcal{T}_{\mathfrak{B}}^6(B, R, R') = \left\{ (\lambda, \mu) \in \mathcal{L}_{\infty}^6(B, R) : \begin{array}{l}
|\mu - 1|_{\mathfrak{B}} < \frac{1}{R'} \text{ or }
|\lambda - 1|_{\mathfrak{B}} < \frac{1}{R} \text{ or }
|\mu - 1|_{\sigma(\mathfrak{B})} < \frac{1}{R'} \text{ or }
|\lambda - 1|_{\sigma(\mathfrak{B})} < \frac{1}{R'} \end{array} \right\}.$$
Proposition 6.15. Let $1 < R_{k+1} < R_k$, $B_k = \left( b^{(k)}_0, b^{(k)}_1, \ldots, b^{(k)}_n \right) \in \mathbb{N}^{n+1}$. Then we have,

$$\mathcal{L}_\infty^6(B_k, R_k) = \mathcal{L}_\infty^6(B_{k+1}, R_{k+1}) \cup \bigcup_{\mathfrak{B} \in S^\infty_\chi \cup S^\infty_\mu} \mathcal{T}_\mathfrak{B}^6(B_k, R_k, R_{k+1})$$

where $b^{(k+1)}_i = \min \left( b^{(k)}_i, c_{1,\infty} \cdot (\log R_{k+1} + c_{2,\infty}) \right)$ for $i \in I^\infty$, otherwise $b^{(k+1)}_i = b^{(k)}_i$, and $c_{2,\infty} = \max_{\mathfrak{B} \in S^\infty_\chi} \left( \sum_{i \notin I^\infty} b^{(k)}_i \log |\lambda_i|_{\mathfrak{B}} \right)$.

Proof. The proof is similar to Proposition 6.7.

We should mention that in this case it may happen that there exists $\mathfrak{B} \in S^\infty_\chi \cup S^\infty_\mu$ such that $|\lambda|_{\mathfrak{B}} = 1$. Then we can not use Lemma 6.1 to prove that the inequality $|\lambda - 1|_{\mathfrak{B}} < \frac{1}{R_{k+1}}$ does not contain non-trivial solutions since the matrix $A$ is non-singular. Let $\sigma_{\mathfrak{B}}$ be the associate to $\mathfrak{B}$ embedding to $\mathbb{R}$ or $\mathbb{C}$. In case $\mathfrak{B}$ be a real place then the condition $|\lambda|_{\mathfrak{B}} = 1$ means that $|\sigma_{\mathfrak{B}}(\lambda)| = 1$ and so $\lambda = \pm 1$. If $\mathfrak{B}$ is a complex place we are not able to eliminate this situation. The only we can do is to apply Lemma 6.1 but expressing $\lambda$ with respect to a basis of the full $S$–unit group. However, this situation seems not to appear quite often in practice.

If we continue this way we reach to a point where we are not able to prove that the sets $\mathcal{T}^j_{\mathfrak{B}}$ do not contain non-trivial solutions. If the bounds and the rank of the groups are small we can just do a simple loop to find all solutions, using these bounds. However, we may still have a lot of cases to consider. We show how we can continue the sieve in the next section.
6.3 Computing solutions

When we can not prove that the sets $T_B$ do not contain non–trivial elements then we have to start computing solutions. The first step is to find congruence solutions $\mod B^e$ of $\mu$ and $\lambda$ for suitable choices of finite primes $B$ and exponents $e$. We do that because computing congruence solutions for a small choice of $e$ can be done quickly since there are very good implementations of discrete logarithm ([Dev16]) and then we have to use only basic linear algebra. In practice we throw away a huge percent of candidate solutions by computing congruence solutions. Then we use Pincke–Pohst algorithm ([FP83]), as Smart and Wildanger do, to determine which lifts of the $\mod B^e$ solutions are solutions of (5.1). After that the remaining solutions have smaller upper bounds for the absolute value of their valuations in prime ideals and we can repeat the procedure we described in the previous section.

Again we take the advantages of Theorems 5.5, 5.6 and 5.7 and the symmetries they introduce in the solutions. As before we consider cases according to the structure of $\mathrm{Gal}(L/K)$.

Let $W$ be the set of pairs $(\lambda, \mu)$ of solutions of (5.1) where $\lambda \in G_\lambda$ and $\mu \in G_\mu$. We define $W_\lambda = \{ \lambda : \lambda \in G_\lambda, \exists \mu \in G_\mu \text{ such that } (\lambda, \mu) \in W \}$. Similarly we define $W_\mu$. For a fixed prime ideal $B \in S_\lambda$ we define

$$b_\lambda = b_\lambda(B) = \max_{\lambda \in W_\lambda} \{|\ord_B(\lambda)|\} \quad b_\mu = b_\mu(B) = \max_{\mu \in W_\mu} \{|\ord_B(\mu)|\}.$$
6.3.1 Quadratic case

In this case we only want to consider congruence solutions for elements in $G_{\lambda}$ because the rank of $G_{\lambda}$ is smaller than the rank\[^3\] of $G_{\mu}$. Let $(\lambda, \mu) \in W$. We recall that $S_{\lambda}$ contains primes $\mathfrak{B}$ which are above primes $p$ of $K$ that split. We fix a prime ideal $\mathfrak{B} \in S_{\lambda}$. We denote by $\tau$ a generator of $\mathrm{Gal}(L/K)$ and $\bar{b}_{\mu} = b_{\mu}(\tau(\mathfrak{B}))$.

**Proposition 6.16.** $b_{\lambda} \leq \max(b_{\mu}, \bar{b}_{\mu})$.

**Proof.** We have to consider three cases.

- If $\text{ord}_{\mathfrak{B}}(\lambda) > 0$ then $\text{ord}_{\mathfrak{B}}(\mu) = 0$. However, we know that $\text{ord}_{\tau(\mathfrak{B})}(\mu) = \text{ord}_{\tau(\mathfrak{B})}(\lambda) = -\text{ord}_{\mathfrak{B}}(\lambda)$. So,

$$|\text{ord}_{\mathfrak{B}}(\lambda)| = |\text{ord}_{\tau(\mathfrak{B})}(\lambda)| = |\text{ord}_{\tau(\mathfrak{B})}(\mu)| \leq \bar{b}_{\mu}.$$

- If $\text{ord}_{\mathfrak{B}}(\lambda) = 0$ then $|\text{ord}_{\mathfrak{B}}(\lambda)| \leq b_{\mu}$.

- If $\text{ord}_{\mathfrak{B}}(\lambda) < 0$ then $\text{ord}_{\mathfrak{B}}(\lambda) = \text{ord}_{\mathfrak{B}}(\mu)$ and we understand that $|\text{ord}_{\mathfrak{B}}(\lambda)| \leq b_{\mu}$.

$\Box$

Proposition 6.16 says that reducing $b_{\mu}$ and $\bar{b}_{\mu}$ we reduce $b_{\lambda}$ too. We will show how we can find new smaller $b_{\mu}$ and $\bar{b}_{\mu}$ by computing solutions in congruence equations. For here and later on we focus only on $\mathfrak{B}$ and $b_{\mu}$. It is important to mention that for a positive integer $e$ and an element $x \in L$ the relation $x \equiv 1 \mod \mathfrak{B}^e$ is equivalent to the inequality $|x - 1|_{\mathfrak{B}} \leq \frac{1}{R}$ where $R = \frac{p}{\mathfrak{B}^e}$, $p$ is the

\[^3\]For this case we have that $G_{\mu} = \mathcal{O}_{L,S_L}$ which does not usually have small rank.
rational prime below $\mathfrak{B}$ and $f_{\mathfrak{B}}$ is the residual degree of $\mathfrak{B}$. For the rest of the section we jump from one form to the other without getting into the details.

Let $e$ be a positive integer which is smaller than $b_\mu$. We want to determine all pairs $(\lambda, \mu) \in W$ such that $|\text{ord}_{\mathfrak{B}}(\mu)| \geq e > 0$. In the case $\text{ord}_{\mathfrak{B}}(\mu) > 0$ we find $\lambda$ using the fact that

$$\lambda \equiv 1 \pmod{\mathfrak{B}^e}.$$ 

On the other hand when $-k := \text{ord}_{\mathfrak{B}}(\mu) \leq -e$ we have that $\text{ord}_{\mathfrak{B}}(\frac{1}{\lambda}) = k$. We define $R = p^{f_{\mathfrak{B}}e}$. Then we see that

$$|\mu|_{\mathfrak{B}} \geq R \iff \left|\frac{1}{\mu}\right|_{\mathfrak{B}} \leq \frac{1}{R} \iff \left|\frac{1}{1 - \lambda}\right|_{\mathfrak{B}} \leq \frac{1}{R} \iff$$

$$\left|1 + \frac{\lambda}{1 - \lambda}\right|_{\mathfrak{B}} \leq \frac{1}{R} \iff 1 \equiv \frac{\lambda}{\lambda - 1} \pmod{\mathfrak{B}^e}$$

We just showed the following proposition.

**Proposition 6.17.** Let $(\lambda, \mu) \in W$ and $\mathfrak{B} \in S_\lambda$ such that $|\text{ord}_{\mathfrak{B}}(\mu)| \geq e > 0$. Then either $\lambda \equiv 1 \pmod{\mathfrak{B}^e}$ or $1 \equiv \frac{\lambda}{\lambda - 1} \pmod{\mathfrak{B}^e}$.

In practice we find the solutions for $x \equiv 1 \pmod{\mathfrak{B}^e}$ and then we check if $x$ corresponds to an element $\overline{x}$ of $\mathcal{O}_{L,S_\lambda}^*$ that satisfies $1 - \overline{x} \in \mathcal{O}_{L,S_\lambda}^*$. We call $\overline{x}$ a lift of $x$. Moreover, by symmetry we have to work only with one of the two conjugate prime ideals $\mathfrak{B}$ and $\tau(\mathfrak{B})$.

### 6.3.2 Cubic case

In the cubic case we know that $G_\lambda = G_\mu$ and we have chosen bases for $G_\lambda$ and $G_\mu$ such that $\mu_i = \sigma(\frac{1}{\lambda})$ for $i = 0, 1, \cdots, n$ where $\sigma$ is a generator of $\text{Gal}(L/K)$. Let $(\lambda, \mu) \in W$ for which we recall that $\sigma(\lambda) = \frac{1}{\mu}$. We fix a prime ideal $\mathfrak{B} \in S_\lambda$. 

79
Proposition 6.18. $b_\lambda = b_\mu$.

Proof. Let $(\lambda, \mu)$ be a pair such that $|\text{ord}_B(\lambda)| > b_\mu$. We know that either $\text{ord}_B(\lambda) = \text{ord}_B(\mu) < -b_\mu$ or $\text{ord}_B(\lambda) > b_\mu$ and $\text{ord}_B(\mu) = 0$. In the first case we understand that $|\text{ord}_B(\mu)| > b_\mu$ which is a contradiction. In the second case the pair $(\frac{1}{\lambda}, -\frac{\mu}{\lambda})$ is an other pair of solutions in $W$ such that $|\text{ord}_B(-\frac{\mu}{\lambda})| = |\text{ord}_B(\lambda)| > b_\mu$ which is a contradiction. So $b_\lambda \leq b_\mu$. By symmetry we have $b_\mu \leq b_\lambda$. \hfill \square

Let $e$ be a positive integer which is smaller than $b_\mu$. We want to determine all pairs $(\lambda, \mu) \in W$ such that $|\text{ord}_B(\mu)| \geq e > 0$.

Proposition 6.19. Let $(\lambda, \mu) \in W$ such that $|\text{ord}_B(\mu)| \geq e > 0$. Then either $\lambda \equiv 1 \mod B^e$ or $\frac{1}{\lambda} \equiv 1 \mod (\sigma(B))^e$.

Proof. Let $R = p^{e/f_B}$ where $p$ is the rational prime below $B$ and $f_B$ the residual degree of $B$. We have that $|\text{ord}_B(\mu)| \geq e \iff |\log|\mu||_B| \geq \log R$. Taking into account that $\sigma(\lambda) = \frac{1}{\mu}$ and $\sigma(\mu) = \frac{\lambda - 1}{\lambda}$ we have that

- $\log|\mu||_B \geq \log R \iff \frac{1}{|\mu||_B} \leq \frac{1}{R} \iff \frac{1}{\lambda} - 1|_{\sigma(B)} | \leq \frac{1}{R}$.
- $\log|\mu||_B \leq -\log R \iff |\mu||_B \leq \frac{1}{R} \iff |\lambda - 1||_B | \leq \frac{1}{R}$.

\hfill \square

We recall that $S_\lambda = S_\mu$ contains primes $B$ which are above primes $p$ of $K$ that split. Let $B_1, B_2, B_3$ be three conjugate prime ideals of $L$ such that $\sigma(B_i) = B_{i+1}$ for $i = 1, 2$ and $\sigma(B_3) = B_1$. By Theorem 5.6 we have that

$$\sum_{i=1}^{3} \text{ord}_{B_i}(\lambda) = \sum_{i=1}^{3} \text{ord}_{B_i}(\mu) = 0.$$
Let \( a_1 = \text{ord}_{B_1}(\lambda) \) and \( a_2 = \text{ord}_{B_2}(\lambda) \). By the above relation and the fact that \( \sigma(\lambda) = \frac{1}{\mu} \) we have

\[
\begin{align*}
    a_1 &= \text{ord}_{B_1}(\lambda) & a_1 + a_2 &= \text{ord}_{B_1}(\mu) \\
    a_2 &= \text{ord}_{B_2}(\lambda) & -a_1 &= \text{ord}_{B_2}(\mu) \\
    -a_1 - a_2 &= \text{ord}_{B_3}(\lambda) & -a_2 &= \text{ord}_{B_3}(\mu)
\end{align*}
\] (6.4)

Proposition 6.20. \( b_\lambda(B_i) = b_\mu(B_j) \) for \( i, j = 1, 2, 3 \).

Proof. By Proposition 6.18 it is enough to show that \( b_\lambda(B_1) = b_\lambda(B_2) \). Assume that there exists a pair \((\lambda, \mu) \in W\) such that \( |\text{ord}_{B_1}(\lambda)| > b_\lambda(B_2) \). We have to consider two cases.

- Suppose that \( \text{ord}_{B_1}(\lambda) > b_\lambda(B_2) \). Then by equations (6.4)–(6.6) we understand that \( a_1 > 0 \) and \( a_2 = -a_1 \). So, we see \( |\text{ord}_{B_1}(\lambda)| = |\text{ord}_{B_2}(\lambda)| \leq b_\lambda(B_2) \).

- Suppose that \( \text{ord}_{B_1}(\lambda) < -b_\lambda(B_2) \). Again by equations (6.4)–(6.6) we conclude that \( a_1 < 0 \) and \( a_2 = 0 \). As a result we understand that \( |\text{ord}_{B_1}(\lambda)| = |\text{ord}_{B_2}(\mu)| \leq b_\mu(B_2) = b_\lambda(B_2) \) by Proposition 6.18.

\( \square \)

Propositions 6.18, 6.19 and 6.20 say that it is enough to find the solutions of \( x \equiv 1 \mod B_1^\epsilon \) and \( x \equiv 1 \mod B_2^\epsilon \) and check which lifts \( \pi \in G_\lambda \) satisfy \( 1 - \pi \in \mathcal{O}_{L,S_L}^\epsilon \).
6.3.3 $S_3$ case

Let $\text{Gal}(L/K) = \langle \sigma, \tau \rangle$ such that $\sigma^3 = \tau^2 = 1$ and $\tau \sigma \tau = \sigma^{-1}$. We recall that we have chosen bases for $G_\lambda$ and $G_\mu$ such that $\mu_i = \sigma(\frac{1}{\lambda})$ for $i = 0, 1, \cdots, n$. Let $(\lambda, \mu)$ be a pair in $W$ for which we have that $\tau(\lambda) = \frac{1}{\lambda}$ and $\sigma(\lambda) = \frac{1}{\mu}$.

We fix a prime ideal $\mathfrak{B}$. We recall that $S_\lambda$ and $S_\mu$ contain prime ideals $\mathfrak{B}$ of $L$ which are above primes $p$ of $K$ that split. Let $g_{\mathfrak{B}}$ be the number of conjugate prime ideals of $\mathfrak{B}$.

**Proposition 6.21.** $S_\lambda$ and $S_\mu$ do not contain prime ideals $\mathfrak{B}$ such that $g_{\mathfrak{B}} = 1, 2$.

**Proof.** The case $g_{\mathfrak{B}} = 1$ has already been considered since we have mentioned at the begin of the chapter that both $S_\lambda$ and $S_\mu$ contain primes $\mathfrak{B}$ which are above split primes of $K$. For $g_{\mathfrak{B}} = 2$ and $\lambda \in S_\lambda$ Theorem 5.7 says that $\text{Norm}_{L/L^*}(\lambda) = \lambda \sigma(\lambda) \sigma^2(\lambda) = -1$. Since $g_{\mathfrak{B}} = 2$ we have that the decomposition group $D_{\mathfrak{B}}(L/K) = \langle \sigma \rangle$. That shows $\text{ord}_{\mathfrak{B}}(\lambda) = 0$. Similarly for $S_\mu$. \[ \square \]

**Case** $g_{\mathfrak{B}} = 3$. Let $\mathfrak{B}_1, \mathfrak{B}_2, \mathfrak{B}_3$ be three conjugate primes such that $\sigma(\mathfrak{B}_i) = \mathfrak{B}_{i+1}$ for $i = 1, 2$, $\sigma(\mathfrak{B}_3) = \mathfrak{B}_1$, $\tau(\mathfrak{B}_1) = \mathfrak{B}_2$ and $\tau(\mathfrak{B}_3) = \mathfrak{B}_3$. By Theorem 5.7 we can deduce that $\mathfrak{B}_1, \mathfrak{B}_2 \in S_\lambda$ and $\mathfrak{B}_3 \not\in S_\lambda$ such that $\text{ord}_{\mathfrak{B}_1}(\lambda) = -\text{ord}_{\mathfrak{B}_2}(\lambda)$. Similarly, $\mathfrak{B}_2, \mathfrak{B}_3 \in S_\mu$ and $\mathfrak{B}_1 \not\in S_\mu$ such that $\text{ord}_{\mathfrak{B}_2}(\mu) = -\text{ord}_{\mathfrak{B}_3}(\mu)$.

From the above we have the following,

**Proposition 6.22.** $b_\lambda(\mathfrak{B}_1) = b_\lambda(\mathfrak{B}_2) = b_\mu(\mathfrak{B}_2) = b_\mu(\mathfrak{B}_3)$. Moreover, we have

$$-\text{ord}_{\mathfrak{B}_1}(\lambda) = \text{ord}_{\mathfrak{B}_2}(\lambda) = -\text{ord}_{\mathfrak{B}_3}(\mu) = \text{ord}_{\mathfrak{B}_2}(\mu) \leq 0.$$
Proof. The relation

\[- \text{ord}_{\mathfrak{B}_1}(\lambda) = \text{ord}_{\mathfrak{B}_2}(\lambda) = - \text{ord}_{\mathfrak{B}_3}(\mu) = \text{ord}_{\mathfrak{B}_4}(\mu) \leq 0,\]

is an immediate consequence of the analysis in the paragraph above the proposition. As a result we have \(b_{\lambda}(\mathfrak{B}_1) = b_{\lambda}(\mathfrak{B}_2) = b_{\mu}(\mathfrak{B}_2) = b_{\mu}(\mathfrak{B}_3).\)

By Proposition 6.22 we understand that it is enough to find solutions of the congruence equation \(x \equiv 1 \mod \mathfrak{B}_5^e\) and check which lifts \(\bar{x} \in G_{\lambda}\) satisfy \(1 - \bar{x} \in \mathcal{O}_{L, S_L}^e.\)

Case \(g_3 = 6.\) Let \(\mathfrak{B}_1, \mathfrak{B}_2, \cdots, \mathfrak{B}_6\) be six conjugate primes such that \(\sigma(\mathfrak{B}_i) = \mathfrak{B}_{i+2}\) for \(i = 1, 2, 3, 4,\) \(\sigma(\mathfrak{B}_5) = \mathfrak{B}_1,\) \(\sigma(\mathfrak{B}_6) = \mathfrak{B}_2,\) \(\tau(\mathfrak{B}_1) = \mathfrak{B}_2,\) \(\tau(\mathfrak{B}_3) = \mathfrak{B}_6\) and \(\tau(\mathfrak{B}_4) = \mathfrak{B}_5.\)

By Theorem 5.7 we deduce that

\[
\begin{align*}
a_1 &= \text{ord}_{\mathfrak{B}_1}(\lambda) = - \text{ord}_{\mathfrak{B}_2}(\lambda) = - \text{ord}_{\mathfrak{B}_3}(\mu) = \text{ord}_{\mathfrak{B}_4}(\mu) \quad (6.7) \\
-a_1 - a_2 &= \text{ord}_{\mathfrak{B}_3}(\lambda) = - \text{ord}_{\mathfrak{B}_4}(\lambda) = - \text{ord}_{\mathfrak{B}_5}(\mu) = \text{ord}_{\mathfrak{B}_6}(\mu) \quad (6.8) \\
a_2 &= \text{ord}_{\mathfrak{B}_5}(\lambda) = - \text{ord}_{\mathfrak{B}_4}(\lambda) = - \text{ord}_{\mathfrak{B}_1}(\mu) = \text{ord}_{\mathfrak{B}_6}(\mu) \quad (6.9)
\end{align*}
\]

Proposition 6.23.

\[
\begin{align*}
b_{\lambda}(\mathfrak{B}_i) &= b_{\lambda}(\tau(\mathfrak{B}_i)) \\
b_{\mu}(\mathfrak{B}_i) &= b_{\mu}(\sigma^2 \tau(\mathfrak{B}_i)) \\
b_{\lambda}(\mathfrak{B}_i) &= b_{\mu}(\sigma(\mathfrak{B}_i))
\end{align*}
\]
for all \( i = 1, \cdots, 6 \).

**Proof.** It is an immediate consequence of the equations (6.7)–(6.9) and the fact that \( \sigma(\lambda) = \frac{1}{\mu} \).

**Proposition 6.24.** Let \((\lambda, \mu) \in W\) such that \(|\text{ord}_B(\mu)| \geq e > 0\). Then either \(\lambda \equiv 1 \mod B^e\) or \(\frac{1}{\lambda} \equiv 1 \mod (\sigma(B))^e\).

**Proof.** It is the same as in Proposition 6.19.

The combination of Propositions 6.23 and 6.24 say that it is enough to find solutions of the congruence equation \(x \equiv 1 \mod B^e\) for \(i = 1, 3, 5\) (or \(2, 4, 6\)) and test which lifts \(\bar{x} \in G_\lambda\) satisfy \(1 - \bar{x} \in \mathcal{O}_{L,S}^*\).

### 6.3.4 Lifting congruence solutions

Even though congruence equations throw away a huge percent of the candidates there are cases where testing all lifts is still expensive. In this section we show a way to reduce the number of candidate lifts. This is based on ideas by Smart and Wildanger ([Sma99], [Wil00], [Wil97], [EG16]).

Let \(B\) be a prime ideal of \(L\), \(e\) a positive integer and \(k\) the exponent of \((\mathcal{O}_K/B^e)^*\). By Lemma 2.16 we can assume \(\lambda = \lambda_0 \prod_{i=1}^n \lambda_i^x_i\) where \(\text{ord}_B(\lambda_i) = 0\) for \(i = 0, \cdots, n\) and \(\lambda_0\) lies in a finite set. We also assume that \(|\log |\lambda|_\mathfrak{Q}| \leq \log R\) for all \(\mathfrak{Q} \in S_\lambda^\infty\) and \(|\text{ord}_\mathfrak{Q}(\lambda)| \leq b_\lambda(\mathfrak{Q})\) for all \(\mathfrak{Q} \in S_{\lambda} \setminus S_{\lambda}^\infty\).

For a fixed \(\lambda_0\) we use discrete logarithm and linear algebra to compute the set \(\Lambda_{0,\text{con}}\) of all elements \(\lambda_0 \prod_{i=1}^n \lambda_i^{x_i} \) with \(0 \leq x_i < k\) which satisfy \(\lambda_0 \prod_{i=1}^n \lambda_i^{x_i} \equiv 1 \mod B^e\) or \(1 \equiv \frac{\lambda_0 \prod_{i=1}^n \lambda_i^{x_i}}{\lambda_0 \prod_{i=1}^n \lambda_i^{x_i-1}} \mod B^e\). We define \(\lambda_{i,k} = \lambda_i^k\) for \(i = 1, \cdots, n\). Then
an element $\lambda \in W_{\lambda}$ is written in the form

$$\lambda = \rho \prod_{i=1}^{n} \lambda_{i,k}^{b_i}$$

where $|t_i| \leq \left\lceil \frac{b_i}{k} \right\rceil + 1$ and $\rho \in \Lambda_{0,\text{con}}$. We define $b_{i,\text{con}} := \left\lceil \frac{b_i}{k} \right\rceil + 1$ for $i = 1, \ldots, n$. We use Fincke–Pohst algorithm to reduce the number of candidate vectors $\vec{t} = (t_1, \cdots, t_n)^t$. For each $\Omega \in S_{\lambda}$ we define

$$r_{\Omega} = \begin{cases} R \cdot \max_{\rho \in \Lambda_{0,\text{con}}} \exp (|\log |\rho||_{\Omega}), & \text{if } \Omega \in S_{\lambda}^\infty \\ p^{b_{\lambda}(\Omega)f_{\Omega}} \max_{\rho \in \Lambda_{0,\text{con}}} \exp (|\log |\rho||_{\Omega}), & \text{if } \Omega \in S_{\lambda} \setminus S_{\lambda}^\infty \end{cases}$$

where $p$ is the rational prime below $\Omega$ and $f_{\Omega}$ the residual degree. Let $\Omega_1, \cdots, \Omega_f$ be the elements of $S_{\lambda}$. We consider the matrix

$$A = \begin{pmatrix} \frac{\log |\lambda_{1,k}|_{\Omega_1}}{\log(r_{\Omega_1})} & \cdots & \frac{\log |\lambda_{n,k}|_{\Omega_1}}{\log(r_{\Omega_1})} \\ \vdots & \ddots & \vdots \\ \frac{\log |\lambda_{1,k}|_{\Omega_f}}{\log(r_{\Omega_f})} & \cdots & \frac{\log |\lambda_{n,k}|_{\Omega_f}}{\log(r_{\Omega_f})} \end{pmatrix} \in \mathbb{R}^{f \times n},$$

**Lemma 6.25.** With the above notation we have that

$$\|Af\|_2^2 \leq f.$$

**Proof.** We have that $|\log |\lambda||_{\Omega} \leq \log R$ for all $\Omega \in S_{\lambda}^\infty$. We know that $\lambda = \cdots$
\[ \rho \prod_{i=1}^{n} \lambda_{i,k}^{t_i} \text{ for some } \rho \in \Lambda_{0,\text{con}}. \] Then it holds

\[
\left| \log \prod_{i=1}^{n} \lambda_{i,k}^{t_i} \right|_{\Omega} = \left| \log \lambda_{i,k}^{t_i} \right|_{\Omega} \leq \left| \log \lambda \right|_{\Omega} + \left| \log |\rho| \right|_{\Omega} \\
\leq \log R + \left| \log |\rho| \right|_{\Omega} \leq \log r_{\Omega}.
\]

Similarly, for \( \Omega \in S_{\lambda} \setminus S_{\lambda}^{\infty} \) we have that \( \left| \log \prod_{i=1}^{n} \lambda_{i,k}^{t_i} \right|_{\Omega} \leq \log r_{\Omega} \). Thus,

\[
\| A\vec{r} \|^2 = \sum_{\Omega \in S_{\lambda}} \frac{\log^2 \left( \prod_{i=1}^{n} |\lambda_{i,k}^{t_i}|_{\Omega} \right)}{\log^2 r_{\Omega}} \leq f.
\]

From Lemma 6.25 we determine all candidate products \( \prod_{i=1}^{n} \lambda_{i,k}^{t_i} \). Multiply all these element with each \( \rho \) and testing \( 1 - \rho \prod_{i=1}^{n} \lambda_{i,k}^{t_i} \in O_{L,S}^{*} \) we determine all solutions of 5.1. See Section 6.4 for a criterion when for a given \( x \in L \) we have \( 1 - x \in O_{L,S}^{*} \).

### 6.3.5 Final step

Now, we know that the absolute value of the exponents of the remaining solutions are smaller. We can repeat the steps of decomposing the set of solutions, as we showed in Section 6.2, and computing solutions with ‘high’ valuation at one prime up to a point where a simple loop is feasible. In practice, it seems that we have to consider congruence equations \( x \equiv 1 \pmod{B^c} \) just once.

In the final simple loop of the \( C_3 \) and \( S_3 \) cases we also use general Hilbert symbols to reduce the number of cases we have to check. Our solutions \((\lambda, \mu)\)
always satisfy \((\lambda \mu_B^\ell)\) for every prime \(\mathfrak{B}\) and integer \(\ell \geq 1\). For a suitable choice of \(\mathfrak{B}\) and \(\ell\) we create the matrix \(A_{\mathfrak{B}} = \left(\left(\frac{\lambda_i \mu_j}{\mathfrak{B}}\right)\right)_{i,j} \in \mathbb{M}_{n+1,n+1}(\mathbb{Z}/\ell\mathbb{Z})\) and we test which vectors exponents \(\vec{x}\) satisfy \(\vec{x}A_{\mathfrak{B}}\vec{x}^t = 0\).

### 6.4 Identifying \(S\)–units efficiently

An expensive part of solving \(S\)–unit equations over a number field \(K\) and a set of prime ideals \(S\) of \(K\) is for given \(x \in K^*\) to determine when \(1 - x \in O_{K,S}^*\). We assume for \(p \in S\) that \(S\) contains all the conjugate of \(p\). We define \(S_Q = \{p \in \mathbb{Z} : \exists p \in S, p | p\}\).

**Lemma 6.26.** Let \(x \in K^*\) and \(f_x(t) \in \mathbb{Q}[t]\) be the minimal polynomial of \(x\) over \(\mathbb{Q}\). It holds \(f_x(1) \in \mathbb{Z}_S^*\) if and only if \(1 - x \in O_{K,S}^*\).

**Proof.** Without loss of generally we assume \(K/\mathbb{Q}\) is Galois and \(\deg f_x = [K : \mathbb{Q}] = n\). We define \(r_x : K \to K\) to be the linear map given by \(r_x(y) = yx\). Let \(A_x = [a_{i,j}]\) be an \(n \times n\) matrix of \(r_x\) associate to a fixed basis of \(K\) over \(\mathbb{Q}\). We know that \(f_x(t) = \det(I - A_x)\) and the conjugate of \(x\) are the eigenvalues of \(A_x\) which are distinct. We denote by \(x := \lambda_1, \cdots, \lambda_n\) the eigenvalues of \(A_x\). Since \(f_x(1) = \det(I - A_x) = \prod_{i=1}^n (1 - \lambda_i)\) we have the result. \(\square\)

Lemma 6.26 is very useful in practise because it seems that there are very good implementations for computing minimal polynomials and testing when an integer is \(S\)–unit than working directly with the \(O_{K,S}^*\) \((\text{Dev16})\).

\(^4\text{We use \textit{tame Hilbert symbol} because there are formulas to evaluate it which are easily implemented compare to the general case. That means we choose only primes in } S_\lambda \cup S_\mu \text{ and } \ell \text{ to be the order of the unit group of the residue field at } \mathfrak{B}.\)
6.5 Example

We continue the case $K = \mathbb{Q}$ and $S = \{2, 3, 23\}$.

**Trivial case.** Using Propositions 5.1, 5.2 and 5.3 we can prove that there does not exist a curve with full 2–torsion that it is not 2–isogenous to a curve without full 2–torsion which has $\lambda$–invariant in one of the 9 quadratic extensions $\mathbb{Q}(\sqrt{d})$ where $d \in \{-1, 2, 3, 6, \pm 23, 46, 69, 138\}$. In other words each curves with full 2–torsion is isogenous to one curve without full 2–torsion which has $\lambda$–invariant in one of the 9 quadratic fields in which we solve an $S$–unit equation.

**Quadratic case.** In the quadratic case we have 9 equations to solve. We will get into the details only for the case $L = \mathbb{Q}(\theta)$, where $\theta^2 = 2$, because the rank of $G_\lambda$ is the maximal among all the 9 fields. We have that

$$G_\lambda = \left[ -1, -2\theta + 3, \frac{10\theta - 27}{23} \right] \quad G_\mu = \left[ -1, \theta - 1, \theta, 3, -\theta + 5, -\theta - 5 \right]$$

Since 23 is the only prime in $S$ which splits in $L$ we have that $S_\lambda$ contains only the two primes $\mathfrak{B}_1$ and $\mathfrak{B}_2$ above 23. On the other hand $S_\mu$ contains all the primes in $L$ above $S$ since $G_\mu = \mathcal{O}_L^{\times,S_L}$ as we mentioned at the begin of the chapter.

By the reduction method we find that 1286 is an upper bound of the absolute value of the exponents of the free part of $G_\lambda$ and $G_\mu$. That means we have $B_0 = (2, 1286, 1286)$ and $C_0 = (2, 1286, 1286, 1286, 1286, 1286)$. We prove that the inequality $|\mu - 1|_{\mathfrak{B}_1} < 23^{-e}$ does not have non–trivial solutions for $e > 16$ and we conclude that $b_\lambda(\mathfrak{B}_1) = b_\lambda(\mathfrak{B}_2) = 16$. Working with the other primes in $S_\mu$ we have $B_1 = (2, 1286, 16)$ and $C_1 = (2, 1286, 82, 16, 16, 25)$.
We continue by applying the results of Section 6.2 and we end up with $B_2 = (2, 45, 16)$ and $C_2 = C_1 = (2, 1286, 82, 16, 16, 25)$. Now the number of candidate $\lambda$ is not so big, just 6005 elements, and we can compute them with a simple loop. At the end we have that

$$W_\lambda = \left\{ \frac{408\theta + 577}{23}, \frac{-2880\theta - 4073}{23}, \frac{-900\theta - 1273}{23}, 12\theta + 17, \frac{1986\theta + 2833}{529}, \frac{-84\theta - 121}{23}, 2\theta + 3, \frac{-24\theta - 41}{23}, \frac{24\theta - 41}{23}, -2\theta + 3, \frac{84\theta - 121}{23}, \frac{-1968\theta + 2833}{529}, -12\theta + 17, \frac{900\theta - 1273}{23}, \frac{2880\theta - 4073}{23}, -408\theta + 577, \frac{-12\theta - 17}{23}, \frac{-2\theta - 3}{23}, \frac{24\theta + 41}{23}, \frac{156\theta + 12169}{12167}, \frac{-540\theta - 929}{23}, 10\theta + 27, \frac{-1}{23}, \frac{-10\theta + 27}{23}, \frac{540\theta - 929}{12167}, \frac{-156\theta + 12169}{23}, \frac{-24\theta + 41}{23}, 2\theta - 3, 12\theta - 17 \right\}$$

From this set of $W_\lambda$ we have the candidate set of $j$–invariants

$$\left\{ \frac{3065617154}{9}, \frac{545138290809}{16928}, \frac{135638288072}{42849}, \frac{287496}{23}, \frac{135559106353}{5037138}, \frac{1488770000}{4761}, \frac{8000}{9}, \frac{2315250}{529}, \frac{2744000}{10976}, \frac{13144256}{4761}, \frac{953312}{529}, \frac{115387499277504}{148035889}, \frac{870436774592}{204004089}, 1728 \right\}$$

Applying Proposition 2.32 we have that all the above candidate $j$–invariants are $j$–invariants of an elliptic curve with good reduction outside $S$.

Working in the same way with the other 8 quadratic extensions and computing $2$–isogenous elliptic curves we compute the set $J_{C_2,1}$ of $j$–invariants of curves over
\[ J_{C_2,1} = \left\{ \frac{2315250}{529}, 8000, \frac{148877000}{4761}, \frac{135559106353}{5037138}, 287496, \frac{135638288072}{42849}, \right. \\
\left. 545138290809, 306567154, 870436774529, 953312, \frac{3930400}{16928}, \frac{9}{9}, \frac{204004089}{2744000}, \frac{529}{529}, \frac{1728}{14283}, \right. \\
\left. 115387499277504, \frac{13144256}{9}, 10976, \frac{115387499277504}{7555707}, 3, \\
\right. \\
\left. 3121792, 413493625, 140608, 19307236, 50591419971625, 19056256, \right. \\
\left. \frac{1587}{1587}, \frac{3}{1587}, \frac{3}{1587}, \frac{28422890688}{27}, \right. \\
\left. 16879645312, 28756228, 10963069081334500, 21081759765625, 949104, \right. \\
\left. 128547, 3, \frac{1156923}{57132}, \frac{529}{529}, \\
\right. \\
\left. 3456, 54000, \frac{1546167879660104}{323754489243}, \frac{839523}{1587}, \frac{14283}{3}, \frac{14283}{14283}, \\
\right. \\
\left. 80919167474, 7301384, 3463512697, 58591911104, 1259712, \frac{23328}{800}, \right. \\
\left. \frac{14283}{3}, \frac{3174}{243}, \frac{529}{529}, \frac{1863}{1863}, \\
\right. \\
\left. \frac{9}{9}, \frac{729}{729}, \frac{23}{23}, \frac{1863}{1863}, \frac{150903}{12223143}, \frac{59049}{59049}, \right. \\
\left. \frac{2924207}{2924207}, \frac{116930169}{28756228}, \frac{21296}{21296}, \frac{314432}{314432}, \frac{17576000}{17576000}, \frac{2924207}{2924207}, \right. \\
\left. \frac{3312}{3312}, \frac{23552}{23552}, \frac{16767}{16767}, \frac{207}{207}, \frac{207}{207}, \frac{16767}{16767}, \frac{81}{81}, \right. \\
\left. \frac{-10627137250000}{-10627137250000}, \frac{4}{4}, \frac{-389017}{-389017}, \frac{-15625}{-15625}, \frac{30289632400448}{-4956477625}, \right. \\
\left. \frac{-110008287}{-110008287}, \frac{9}{9}, \frac{828}{828}, \frac{207}{207}, \frac{58194383823}{58194383823}, \frac{268272}{268272}, \\
\right. \\
\left. \frac{752329532375}{752329532375}, 107850176, 3370318, 1666957239793, 209254946, 65939264, \right. \\
\left. \frac{448524288}{448524288}, \frac{16767}{16767}, \frac{81}{81}, \frac{301806}{301806}, \frac{207}{207}, \frac{1863}{1863}, \right. \\
\left. \frac{7377976076947776}{7377976076947776}, 2491343456, 13289344, 12214672127, 4499456, 2048, \right. \\
\left. \frac{12167}{12167}, \frac{1358127}{1358127}, \frac{23}{23}, \frac{9}{9}, \frac{27}{27}, \frac{3}{3}, \\
\right. \\
\left. \frac{61604313088}{61604313088}, 15043017316604, 3538944, 6859000, 13783349619074, 51478848, \right. \\
\left. \frac{621}{621}, \frac{243}{243}, \frac{23}{23}, \frac{3}{3}, \frac{69}{69}, \frac{23}{23}, \\
\right. \\
\left. 0, \frac{545338513}{545338513}, 1556068, 170769126592, \frac{-8000}{128}, \frac{4135997648}{128}, \frac{4000}{81}, \frac{21952}{81}, \right. \\
\left. \frac{-219488}{-219488}, \frac{35152}{35152}, \frac{676449508}{676449508}, \frac{64}{64}, \frac{-873722816}{-873722816}, \frac{207646}{207646}, \frac{97336}{97336}, \right. \\
\left. \frac{729}{729}, \frac{9}{9}, \frac{4761}{4761}, \frac{9}{9}, \frac{59049}{59049}, \frac{6561}{6561}, \frac{81}{81} \right\} \\

\text{At the end we have 97 isomorphism classes with 1664 elliptic curves. The}^{5}\text{We include curves for } j = 0, 1728. \text{ For } j = 0 \text{ there are curves with good reduction outside } \{2, 3, 23\} \text{ but } \#E(\mathbb{Q})[2] = 1.
maximal conductor is $1218816 = 2^8 3^2 23^2$.

**Cubic case.** We have shown that there is only one cubic extension over $\mathbb{Q}$ unramified outside $S$ which is the splitting field of the polynomial $x^3 - 3x - 1$. We define $L = \mathbb{Q}(\phi)$ such that $\phi^3 - 3\phi - 1 = 0$. We have that

$$G_\lambda = [-1, \phi^2 - \phi - 1, \phi + 1] \quad \quad G_\mu = [-1, -\phi, \phi^2 - 2]$$

All the generators of $G_\lambda$ and $G_\mu$ are in $\mathcal{O}_K^*$. By the reduction step we have that $35$ is an upper bound of the absolute value of the exponents of the free part of $G_\lambda$ and $G_\mu$. So, $B_0 = (2, 35, 35)$. Since $S_\lambda$ and $S_\mu$ do not contain prime ideals we go directly to reduce the upper bound for the unit generators while $B_1 = B_0$. Applying the results of Section 6.2 we get that $B_2 = (2, 14, 14)$ and there are 1681 candidates for $\lambda$. Then a simple loop computes $W_\lambda$ which is

$$W_\lambda = \{ 21\phi^2 - 7\phi - 60, -2\phi^2 + \phi + 6, \phi^2 - 2, -\phi^2 + \phi + 2, \phi^2 - 2\phi, -14\phi^2 + 21\phi + 10, \phi^2 + \phi, -\phi, -7\phi^2 - 14\phi - 4 \}$$

From this set of $W_\lambda$ the candidate set of $j$–invariants is

$$\{ 790272, 6912, 2304 \}$$

Again by Proposition 2.32 we have that all the above candidate $j$–invariants are $j$–invariants of an elliptic curve with good reduction outside $S$. So, we have 3 isomorphism classes with 48 curves and maximal conductor $2742336 = 2^6 3^4 23^2$.

---

In practice it seems that we get ‘small’ upper bounds from the reduction step when all the generators of $G_\lambda$ and $G_\mu$ lie in $\mathcal{O}_K^*$. 
$S_3$ case. In this case we have 37 equations to solve. We will present the details of the case where \( \text{rank}(G_{\lambda}) = \text{rank}(G_{\mu}) \) is the highest. This is the case where 

\( L \) is the splitting field of the polynomial \( x^3 - 6x - 3 \). As \( L/\mathbb{Q} \) is a tower of a quadratic and cubic extension then we have \( L = \mathbb{Q}(\xi, \psi) \) where \( \psi^2 - 69 = 0 \) and \( \xi^3 - 6\xi - 3 = 0 \). We have that

\[
G_{\lambda} = \left[ -1, -\frac{4}{69} \psi \xi^2 + \left( \frac{1}{23} \psi + 1 \right) \xi + \frac{3}{46} \psi + \frac{1}{2}, \left( -\frac{3}{23} \psi + 3 \right) \xi^2 + \left( \frac{8}{23} \psi - 6 \right) \xi + \frac{1}{46} \psi - \frac{11}{2}, \left( -\frac{1}{276} \psi + \frac{1}{4} \right) \xi^2 + \frac{3}{46} \psi \xi + \frac{9}{92} \psi - \frac{5}{4}, \left( \frac{15}{23} \psi - \frac{63}{23} \right) \xi^2 + \frac{28}{23} \psi + \frac{168}{23} \right]
\]

\[
G_{\mu} = \left[ -1, -\frac{4}{69} \psi \xi^2 + \left( -\frac{1}{23} \psi - 1 \right) \xi - \frac{3}{46} \psi + \frac{1}{2}, \left( -\frac{9}{23} \psi - 3 \right) \xi^2 + \left( \frac{1}{23} \psi + 3 \right) \xi + \frac{95}{46} \psi + \frac{37}{2}, \left( \frac{1}{69} \psi - \frac{1}{2} \right) \xi^2 + \left( -\frac{1}{92} \psi + \frac{1}{4} \right) \xi - \frac{13}{92} \psi + \frac{7}{4}, \left( \frac{18}{23} \psi + \frac{132}{23} \right) \xi^2 + \frac{14}{23} \psi - \frac{30}{23} \right]
\]

By the reduction step we have that 663 is an upper bound of the absolute value of the exponents of the free part of \( G_{\lambda} \) and \( G_{\mu} \). So, \( B_0 = (2, 663, 663, 663, 663) \).

There are 3 primes above 2 and 23 and one prime above 3 in \( L \). Thus \( g_B = 3 \) for all \( B \in S_{\lambda}, S_{\mu} \). By proving the non–existence of solutions of the inequality \( |\mu - 1|_B < \delta \) for suitable choice of \( B \in S_{\lambda} \setminus S_{\mu} \) and \( \delta \) we have that \( B_1 = (2, 663, 663, 64, 31) \).

We continue by applying the results of Section 5.2 and we end up with \( B_2 = (2, 247, 226, 64, 31) \). Now we are not able to prove that all the sets \( T^B_6 \) are empty and the number of cases we have to check is too big\(^7\) to allow us to do a simple loop. We continue by computing solutions such that \( \mu \equiv 1 \mod (B_2)^4 \) where

\(^7\) With the upper bound \( B_0 \) the number of candidate solutions is \( \sim 3 \times 10^{12} \) while after applying the results of Section 5.2 we have \( B_1 \) and the number has been decreased to \( \sim 3.6 \times 10^9 \).
$\mathfrak{B}_2|2$ and $\mathfrak{B}_2 \in S_\lambda \setminus S_\mu$. We find 10 solutions and only 7 out of them give $j \in \mathbb{Q}$. These $j$'s are

$$\{ 6848175699/1472, 1860867/368, 651245403/376832, 149721291/48668, 1167051/23, 311469, 1601613/64 \}.$$ 

Now we have $B_3 = (2, 247, 226, 4, 31)$. The next step if to find solutions such that $\mu \equiv 1 \mod (\mathfrak{B}_{23})^2$ where $\mathfrak{B}_{23} | 23$ and $\mathfrak{B}_{23} \in S_\lambda \setminus S_\mu$. We find 5 solutions with the following $j$'s

$$\{ 620663201409024/3404825447, 121697237568/12167, 23892339312/6436343, 618470208/12167, 107986944/12167 \}.$$ 

Now $B_4 = (2, 247, 226, 4, 2)$ and we can apply again the results of Section 6.2. After that we have that $B_5 = (2, 57, 57, 4, 2)$ and a simple loop is now feasible. The remaining solutions are 13 with $j$'s


To sum up we have 25 candidate $j$'s and by Proposition 2.32 we can see that all the above candidate $j$–invariants are $j$–invariants of an elliptic curve with good reduction outside $S$.

Working in the same way with the rest 36 $S_3$ extensions where the rank of $G_\lambda$
and $G_\mu$ are smaller we compute the set $J_{S_3}$ of $j$–invariants of elliptic curves with good reduction outside $S$ and 6 degree 2–division field.

$$J_{S_3} = \left\{ \begin{array}{c}
-605310849 \\
1024
-149122432 \\
59049
-3306921612804657 \\
8875147264
-316368 \\
4
-42592000 \\
12167
-2164528 \\
279841
-188416 \\
23
-820125 \\
529
-1990656 \\
529
-41472 \\
279841
-4269861568512 \\
423
-121697237568 \\
12167
-1167051 \\
23
-46656 \\
23
-90855097472 \\
23
-6718464 \\
23
-55699202259 \\
23
-25745372 \\
8
\end{array} \right\}
\begin{array}{c}
207 \\
-26496 \\
-152827456 \\
-820125 \\
-41472 \\
-1152 \\
-149984000 \\
-972 \\
-6144 \\
-9553393300769782272 \\
-663552 \\
-37897187584 \\
-382944 \\
-3556224000 \\
-23
-140625 \\
-60466176 \\
-64 \\
-1860867 \\
-576 \\
-49152 \\
-23
-37044 \\
-4408272 \\
-2817559698624 \\
989120151 \\
92
-1550640289 \\
1327104 \\
-1472 \\
-15944049 \\
766656 \\
109503 \\
41472 \\
-9936 \\
1472 \\
-121697237568 \\
105456 \\
8 \\
1083392 \\
8 \\
128
\end{array} \right\}.$$
Again by Proposition 2.32 we have that all the above candidate $j$–invariants are $j$–invariants of an elliptic curve with good reduction outside $S$. So, we have 213 isomorphism classes with 3808 curves and maximal conductor $3290832 = 2^83^523^2$. 

To sum up, for $K = \mathbb{Q}$ and $S = \{2, 3, 23\}$ we have found 312 isomorphism classes and 5520 curves.

8Including $j = 0$.

9$j = 0$ appears both in the $C_2$ and $S_3$ cases.
We have to mention that we did all the computations in a modern server and the code has been written in Sage ([Dev16]). The whole amount of time was around 8 hours where 6 minutes 6 seconds was the computation for $J_{C_1,2}$, 4 seconds for $J_{C_3}$ and the remaining time for $J_{S_3}$. Among the 37 fields in $S_3$ case the field we presented in the example above was the most expensive, around 6 hours. The most expensive part was when we had to check that a big amount of candidates $\lambda$ or $\mu$ satisfied $1 - \lambda$ or $1 - \mu$ be a $S$–unit. That happens when we test lifts of congruence solutions (see Section 6.3.4) and at the final loop (see Section 6.3.5).

Moreover, we have compared the above results with other methods and all find the same set of curves. The version of Sage where the implementation was written ([Dev16]) includes an implementation of Cremona–Lingham method ([CL07]). It took around 19 hours to compute the curves in the same server as in our method while the input variable proof of the corresponding function[^96] was in False mode. The effect of ‘proof=False’ is that when the function needs to find $S$–integral points on a curve it does not worry when it is not able to compute a basis of the Mordell–Weil group. The use of ‘proof=False’ speeds up the implementation but it does not guarantee the completeness. However, in practice we expect not to miss curves.

An other implementation is by John Cremona and Ariel Pacetti based on [CPV16]. The approach of the method is different and it is based on computing orders in quadratic and cubic extensions and solutions on Thue equations. However, the method uses an explicit version of ABC conjecture ([Sil86, VIII.11.4]) to bound the index of the orders. The implementation is in Pari/GP ([PAR16])

[^96]: The name of the function is EllipticCurves_with_good_reduction_outside_S.
and it took around 30 min to compute the same set of curves in a similar server as in the above methods.

Finally, the last implementation is due to Michael Bennett and Andrew Richnitzer based on [BR16]. This method combines classical invariant theory of cubics forms and solutions of Thue equations. The details of the implementation and the computer power can be found in [BR16] while the time for the computations was around 20 minutes.
Chapter 7

Conclusion

At the end of this thesis we would like to make some final remarks. The big advantage of solving $S$–unit equations for computing $E_{K,S}$ is that we have a method which both the theory and the implementation work over every number field and the method gives complete set of curves. It does not depend on any conjecture and at the end of the day we just have to do a finite search which may be huge but is still finite!

On the other hand we have to do computations on high degree extensions since we work on the 2–division field. Everywhere in this thesis we made the assumption that computing bases of $S$–unit groups is doable. However, this is not always true when the degree of the field is high or we have a lot of primes or primes with big norm.

An other important factor that would make faster this method would be a better implementation. The necessity of this thesis forced us to write thousand lines of code which implemented the ideas of De Weger, Tzanakis, Smart and Wildanger ([Weg88], [Weg87], [TdW89], [TW92], [Sma95], [Sma98], [Sma99], [Wil00], [Wil00].
We hope that this code or a part of it will be included in a future version of Sage. However, $S$–unit equations have a lot of applications in number theory and we believe that it is worthy to translate this code or part of it in a lower level language, like Pari/GP or C.

We strongly believe that the approach of this thesis for computing $\mathcal{E}_{K,S}$ by using the $\lambda$–invariant can be extended to higher genus curves, e.g. genus 2 and Picard curves. However, the geometry in high genus curves is more complicated and different than genus 1 curves.

Finally, we want to mention that we have used the method of this thesis to compute sets $\mathcal{E}_{K,S}$ of curves for a variety of sets of primes $S$ when $K = \mathbb{Q}$ or a quadratic field. You can find the results of the computations in the homepage\footnote{The homepage may have changed.} of the author,

[https://sites.google.com/site/angeloskoutsianas/](https://sites.google.com/site/angeloskoutsianas/)

or you can contact to koutsis.jr@gmail.com.
Bibliography


