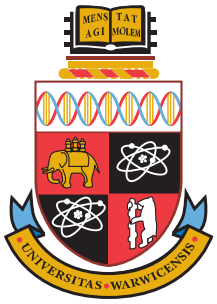

Applications of S-unit Equations to the Arithmetic of Elliptic Curves

by

Angelos Koutsianas

Thesis

Submitted to the University of Warwick

for the degree of

Doctor of Philosophy

Mathematics Institute

September 2016

THE UNIVERSITY OF WARWICK

Στη σύζυγό μου Κέλλυ
και στον γιο μου Κωνσταντίνο

Contents

Acknowledgements

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, Rosemberg 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 λ–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 $\mathcal{O}^*_{L,S_L}$ 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

$$\mathcal{O}^*_{L,K,S_L,1} = \{x \in \mathcal{O}^*_{L,S_L} | \operatorname{Norm}_{L/K}(x) = 1\}$$
$$\mathcal{O}^*_{L,K,S_L,\pm 1} = \{x \in \mathcal{O}^*_{L,S_L} | \operatorname{Norm}_{L/K}(x) = \pm 1\}$$
$$\mu = 1 - \lambda$$
$$j = 2^8 \frac{(\lambda^2 - \lambda + 1)^3}{\lambda^2 (1-\lambda)^2}$$
$$w = j^2 (j - 1728)^3$$

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, λ and μ are solutions of the S–unit equation

$$\lambda + \mu = 1$$

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

- *Suppose $\operatorname{Gal}(L/K) = C_2$, then $\lambda \in \mathcal{O}^*_{L,K,S_L,1}$ and $\mu \in \mathcal{O}^*_{L,S_L}$,*
- *Suppose $\operatorname{Gal}(L/K) = C_3 = \langle \sigma \rangle$, then $\lambda \in \mathcal{O}^*_{L,K,S_L,\pm 1}$ and $\sigma(\lambda) = \frac{1}{\mu}$,*
- *Suppose $\operatorname{Gal}(L/K) = S_3 = \langle \sigma, \tau \rangle$ such that $\sigma^3 = \tau^2 = 1$ and $\tau\sigma\tau = \sigma^{-1}$.*

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

Conversely, let assume that $\mathrm{Gal}(L/K)$ *is not trivial and* j, w, μ *as above. If* λ *and* μ *satisfy the above conditions, according to the structure of* $\mathrm{Gal}(L/K)$*, 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* $S \cup \{\mathfrak{p} \subset \mathcal{O}_K : \mathfrak{p} \mid 3\}$*.*

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 λ and μ 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 $\mathcal{O}_{K_\mathfrak{p}}$,

- $k_{\mathfrak{p}}$ the residue field of $\mathcal{O}_{K_{\mathfrak{p}}}$,
- E(or E/F) an elliptic curve defined over a field F.

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

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3 \tag{2.1}$$

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 $K_{\mathfrak{p}}$) such that $a_1, \cdots, a_6 \in \mathcal{O}_K$ (or $\mathcal{O}_{K_{\mathfrak{p}}}$) then (2.1) is called an *integral Weierstrass equation* of E. In general, we write the Weierstass equation of E using the non–homogeneous coordinates $x = \frac{X}{Z}$ and $y = \frac{Y}{Z}$,

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \tag{2.2}$$

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

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

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

We define the quantities

$$b_2 = a_1^2 + 4a_2, \qquad b_4 = 2a_4 + a_1a_3, \qquad b_6 = a_3^2 + 4a_6,$$

$$\begin{aligned} b_8 &= a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2, \\ c_4 &= b_2^2 - 24b_4, \\ c_6 &= -b_2^3 + 36b_2b_4 - 216b_6, \\ \Delta &= -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6, \\ j &= \frac{c_4^3}{\Delta}. \end{aligned}$$

We can easily verify the relations

$$4b_8 = b_2b_6 - b_4^2, \qquad 1728\Delta = c_4^3 - c_6^2.$$

The quantity Δ is called the *discriminant* of the Weierstrass equation and j the *j–invariant* of E.

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

$$E : y^2 = 4x^3 + b_2x^2 + 2b_4x + b_6. \tag{2.3}$$

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

$$E : y^2 = x^3 - 27c_4x - 54c_6 \tag{2.4}$$

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 $\overline{F}$ *if and only if they have the same* j*–invariant.*

(iii) Let $j_0 \in \overline{F}$. *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

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

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 $nP = \overbrace{P + P + \ldots + P}^{n\text{-times}}$. 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

$$E[n] = \big\{P \in E(\overline{F}) : nP = \mathcal{O}\big\}$$

The following theorem holds,

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

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

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

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

  (i) $E[p^e] \simeq \{\mathcal{O}\}$ *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 $\phi : E_1 \longrightarrow E_2$ 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 ϕ, denoted $\deg\phi$, is its degree as a finite map of curves. If $\mathrm{char}\, F = 0$ then $\deg\phi = \#\phi^{-1}(\mathcal{O}_{E_2})$. For

each isogeny ϕ there is an isogeny $\hat{\phi} : E_2 \longrightarrow E_1$ 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 ϕ.

Example: Assuming that $\operatorname{char} F \neq 2$ 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,

$$\begin{aligned} &\phi : E_1 \longrightarrow E_2 && \hat{\phi} : E_2 \longrightarrow E_1, \\ &(x, y) \longmapsto \left(\frac{y^2}{x^2}, \frac{y(b - x^2)}{x^2} \right) && (X, Y) \longmapsto \left(\frac{Y^2}{4X^2}, \frac{Y(r - X^2)}{8X^2} \right). \end{aligned}$$

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

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* $\operatorname{char}(F) \neq 2, 3$.

(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_λ *is*

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

(iii) The map

$$\overline{F} \setminus \{0, 1\} \longrightarrow \overline{F}, \qquad \lambda \longmapsto j(E_\lambda),$$

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 λ*–invariant* λ *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_λ.

Even though we define λ–invariant using the roots of $f_{2,E}$ which depend on the model we have chosen, Theorem 2.5 says that λ is independent of the model of E. Moreover, one can show that λ 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 $\Lambda := \left\{\lambda, 1 - \lambda, \frac{1}{\lambda}, \frac{1}{1-\lambda}, \frac{\lambda}{\lambda - 1}, 1 - \frac{1}{\lambda}\right\}$ 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 λ 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[1] $K_\mathfrak{p}$ 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_K^0 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 $\prod_{\mathfrak{p}\in M_K^0} \mathfrak{p}^{v_\mathfrak{p}(\Delta_\mathfrak{p})}$. Fixing a Weierstrass model of E over K with

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

discriminant Δ, there exists $u_{\mathfrak{p}} \in K$ for each $\mathfrak{p} \in M_K^0$ such that $\Delta = u_{\mathfrak{p}}^{12}\Delta_{\mathfrak{p}}$. If we define $\mathfrak{a}_\Delta = \prod_{\mathfrak{p}\in M_K^0} \mathfrak{p}^{-v_{\mathfrak{p}}(u_{\mathfrak{p}})}$ then it holds

$$\mathcal{D}_{E/K} = (\Delta)\mathfrak{a}_\Delta^{12}.$$

One can show that the ideal class $\bar{\mathfrak{a}}_{E/K}$ of $\mathfrak{a}_\Delta$ is independent of the Weierstrass model for E and $\bar{\mathfrak{a}}_{E/K}$ 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 $\mathcal{D}_{E/K} = (\Delta)$.

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

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 $\mathfrak{p}$ (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 can not 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 $\mathfrak{p}$ if and only if E_2 has good reduction at $\mathfrak{p}$.*

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 $\mathrm{Twist}\,((E,\mathcal{O})/K)$.

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

$$E^{(d)} : y^2 = x^3 + a_2dx^2 + a_4d^2x + d^3a_6 \tag{2.5}$$

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 $\mathrm{Twist}\,((E,\mathcal{O})/K)$.

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 $\text{Twist}\,((E,\mathcal{O})/K)$ *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*

$$\begin{array}{lll} (i) & y^2 = x^3 + d^2Ax + d^3B & \text{if } j \neq 0, 1728, \\ (ii) & y^2 = x^3 + dAx & \text{if } j = 1728, \\ (iii) & y^2 = x^3 + dB & \text{if } j = 0. \end{array}$$

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[2] *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

$$\mathcal{O}_{K,S} = \{x \in K : v_{\mathfrak{p}}(x) \geq 0, \forall \mathfrak{p} \notin S\}$$
$$\mathcal{O}_{K,S}^* = \{x \in K : v_{\mathfrak{p}}(x) = 0, \forall \mathfrak{p} \notin S\}$$

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

$$\mathcal{O}_{K,S}^* = \mathcal{O}_K^* \oplus \bigoplus_{i=1}^{\#S} \mathbb{Z}\gamma_i \tag{2.6}$$

where $\gamma_i \notin \mathcal{O}_K^*$.

We say that an ideal I of K is *S–integral* if $v_{\mathfrak{p}}(I) \geq 0$ for all $\mathfrak{p} \notin S$. 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*

$$C\ell_S(K) \simeq C\ell(K)/\langle \bar{\mathfrak{p}} \rangle_{\mathfrak{p} \in S}$$

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

Proof. See [Coh00, Proposition 7.4.4]. □

For a positive natural integer n we define the *n–Selmer group of K and S* to

be

$$K(S,n) = \{x \in K^*/K^{*n} : v_{\mathfrak{p}}(x) \equiv 0 \mod n, \forall \mathfrak{p} \notin S\}.$$

The *n–Kummer exact sequence of $\mathcal{O}_{K,S}^*$* holds:

$$1 \to \mathcal{O}_{K,S}^*/\mathcal{O}_{K,S}^{*n} \to K(S,n) \xrightarrow{a_n} C\ell_S(K)[n] \to 1$$

where $C\ell_S(K)[n]$ is the n–torsion subgroup of $C\ell_S(K)$ and the map $a_n : K(S,n) \to C\ell_S(K)[n]$ 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 $(u,v) \mapsto v^{am}u^{bn}$ such that $am + bn = 1$.

Proof. See [CL07, Proposition 2.1]. □

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

$$\mathcal{O}_{L,K,S_L,1}^* = \{x \in \mathcal{O}_{L,S_L}^* \,|\, \mathrm{Norm}_{L/K}(x) = 1\}$$
$$\mathcal{O}_{L,K,S_L,\pm 1}^* = \{x \in \mathcal{O}_{L,S_L}^* \,|\, \mathrm{Norm}_{L/K}(x) = \pm 1\}$$

Finally, for a place $\mathfrak{p}$ of K we define its absolute value to be,

$$|x|_{\mathfrak{p}} = \begin{cases} p^{-f_{\mathfrak{p}} v_{\mathfrak{p}}(x)}, & \text{if } \mathfrak{p} \text{ is a finite prime.} \\ |\sigma_{\mathfrak{p}}(x)|, & \text{if } \mathfrak{p} \text{ is an infinite real prime.} \\ |\sigma_{\mathfrak{p}}(x)|^2, & \text{if } \mathfrak{p} \text{ is an infinite complex prime.} \end{cases}$$

where $\sigma_{\mathfrak{p}}$ is the associated embedding into $\mathbb{R}$ or $\mathbb{C}$ when $\mathfrak{p}$ is an infinite place and $f_{\mathfrak{p}}$ is the residual degree and p the rational prime below $\mathfrak{p}$ when $\mathfrak{p}$ 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 μ_n is the group of the n–th roots of unity of $\overline{F}$. The *general Hilbert symbol of F with respect to n* is a nondegenerate bilinear pairing

$$\left(\frac{\cdot,\cdot}{F}\right)_n : F^*/F^{*n} \times F^*/F^{*n} \longrightarrow \mu_n.$$

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) $\left(\frac{ab,c}{F}\right)_n = \left(\frac{a,c}{F}\right)_n \left(\frac{b,c}{F}\right)_n$.

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

(iii) $\left(\frac{a,b}{F}\right)_n = 1 \Leftrightarrow a$ *is a norm for the extension* $F(\sqrt[n]{b})/F$.

(iv) $\left(\frac{a,b}{F}\right)_n = \left(\frac{b,a}{F}\right)_n^{-1}$.

(v) $\left(\frac{a,1-a}{F}\right)_n = 1$ *and* $\left(\frac{a,-a}{F}\right)_n = 1$.

(vi) if $\left(\frac{a,b}{F}\right)_n = 1$ *for all* $b \in F^*$ *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 $K \hookrightarrow K_{\mathfrak{p}}$ allows us to define *general Hilbert symbol of* K *with respect to* $\mathfrak{p}$ *and* n.

For a number field K we define the map $\left(\frac{\cdot}{K}\right) : K^*/K^{*2} \times K^*/K^{*2} \longmapsto \mu_2$ such that $\left(\frac{a,b}{K}\right) = 1$ 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* $\mathrm{Gal}(K(f)/K) \subset A_n$ *if and only if* $\Delta(f)$ *is a square in* K.

Proof. See [Coh93, Proposition 6.3.1]. □

Let $G = \langle g_0, g_1, \cdots, g_n \rangle$ 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 $i = 0, 1, \cdots, n$ 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 $i = 0, 1 \cdots, s_n$ such that*

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

(ii) $s_n = n$ *if* $\mathrm{ord}_{\mathfrak{p}}(g_i) = 0$ *for all* $i = 0, 1, \cdots, n$ *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]. □

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 $e_{\mathfrak{p}}$ and $f_{\mathfrak{p}}$ the ramification and residual degree of $\mathfrak{p}$. Let $q = p^{f_{\mathfrak{p}}}$. For an element $x \in K_{\mathfrak{p}}$ we define

$$\mathrm{ord}_p(x) = \frac{\mathrm{ord}_{\mathfrak{p}}(x)}{e_{\mathfrak{p}}}.$$

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

$$|x|_p = p^{-\mathrm{ord}_p(x)}.$$

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 $L_{\mathfrak{p}}$ of $K_{\mathfrak{p}}$.

For an element $x \in K_{\mathfrak{p}}$ 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 $x \in K_{\mathfrak{p}}$ such that $|x|_p = 1$ in the following way. Let o be the multiplicative order of x modulo $\mathfrak{p}$. We choose t such that $p^t > e_{\mathfrak{p}}$ then one can show that $\mathrm{ord}_p(1-x^{op^t}) > 1$. 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 $x, y \in K_{\mathfrak{p}}$ such that $|x|_p = |y|_p = 1$ we have $\log_p(xy) = \log_p(x) + \log_p(y)$. For an element x that satisfies $|x|_p < p^{-\frac{1}{p-1}}$ it also holds

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

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 $\mathrm{Gal}(L/K)$ is an abelian group. If $\mathrm{Gal}(L/K)$ is a cyclic group then the extension is called *cyclic*. In this section we explicitly describe all cyclic extensions of K of prime degree ℓ, and those which are unramified outside a given set of prime ideals S of K.

The case $\zeta_n \in K$

Let K be a number field and ζ_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 $G_K = \mathrm{Gal}(\overline{K}/K)$ the Galois group of the algebraic closure of K then*

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

Proof. See [NSW08, Theorem 6.2.2] □

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]. □

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, ℓ 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 $\mathfrak{p} \mid \ell$ and the congruence*

$$x^\ell \equiv a \mod \mathfrak{p}^{z(\mathfrak{p},\ell)-1+v_\mathfrak{p}(a)}$$

has a solution in K.

Proof. See [Coh00, Corollary 10.2.12]. □

Corollary 2.20. *Let K be a number field, ℓ 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 $K(S, \ell)$. □

The case $\zeta_n \notin K$

The situation is more complicated when $\zeta_n \notin K$. We have to adjoin ζ_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 $\mathrm{Gal}(L_1L_2/L_2)$ and $\mathrm{Gal}(L_1L_2/L_1)$, respectively. Moreover, $G_1 \simeq \mathrm{Gal}(L_1L_2/L_2)$ 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 ℓ. 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 $G_{K_z} = \mathrm{Gal}(K_z/K)$ is generated by the automorphism τ 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 τ acts as an endomorphism t of W, of order dividing d. Since $d \mid (\ell-1)$ hence is coprime to ℓ, 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 $W = \oplus_{0\le k<d} W_k$, where W_k is the eigenspace corresponding to the eigenvalue g^k of τ.

For $0 \leq k < d$ we define,

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

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 $\zeta_\ell \notin K$ with $W = K_z^*/K_z^{*\ell}$.

Theorem 2.24. *Let K be a number field and L an abelian extension of K of degree ℓ. Assume that $\zeta_\ell \notin K$, $K_z = K(\zeta_\ell)$ and $L_z = L(\zeta_\ell)$. Let g_0 be a primitive root modulo ℓ, $d = [K_z : K] = \frac{l-1}{m}$ and $g = g_0^m$ as above. Finally, let $W = K_z^*/K_z^{*\ell}$.*

(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

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

where τ is any extension to L_z of the K–automorphism τ of K_z.

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

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

(iv) We have

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

(v) Conversely, if we are given a abelian extension L of K of prime degree ℓ by $L = K(\eta)$ and if we define θ 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 τ to L_z/K. We define $\lambda_0 = \sum_{0 \le i < d} g^{d-1-i}\tau^i$. For any element λ in $\mathbb{Z}[G_z]$ such that $\lambda \equiv \lambda_0 \mod \ell$, hence both g and m are coprime to ℓ, we have that $\bar{\lambda} \equiv ce_1 \mod \ell$ for some $c \in \mathbb{F}_\ell^*$. Since W is a $\mathbb{F}_\ell$–vector space, we have that $e_1 W = \bar{\lambda} W$. By the definition of W_1 we have that $\tau(a) = a^g \gamma^\ell$ for some $\gamma \in K_z^*$. Since $W_1 = e_1 W$, by Proposition 2.23, we have $W_1 = \bar{\lambda} W$ and we understand that $a = \beta^\lambda \delta^\ell$ for some $\beta \in K_z^*$.

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*

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

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

Conversely, let β be given such that $a = \beta^\lambda$ and let $\lambda = \lambda_0 + \nu\ell$ for $\nu \in \mathbb{Z}[G_z]$ and λ_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 $\tau(\theta) = \theta^{g}\beta^{\mu}$.*

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 $a = \beta^{\lambda}\delta^3$ for some $\delta \in K_z^*$. If $\delta = 1$ Corollary 2.26 says that $\tau(\theta) = \theta^{g}\beta^{\mu} = \frac{\theta^2}{\beta}$ and by Theorem 2.24 we have a defining polynomial of L/K to be

$$P(X) = X^3 - 3eX - e\,\mathrm{Tr}_{K_z/K}(\beta)$$

where $e = \mathrm{Norm}_{K_z/K}(\beta)$.

2.5 Lattices

Let n be a positive integer. A *lattice* $\mathcal{L}$ 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* $\mathcal{L}$. Formally $\mathcal{L}$ is of the form

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

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

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* $\vec{b}_1, \cdots, \vec{b}_n$ *and inner product* $\langle , \rangle$ *has a orthogonal basis given by* $\vec{b}_1^*, \cdots, \vec{b}_n^*$ *where*

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

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

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

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

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]. □

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]. □

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

$$ax + by = 1 \tag{2.7}$$

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 $\mathcal{E}_{K,S}$.

Cremona and Lingham show that for computing $\mathcal{E}_{K,S}$ it is enough to determine the j–invariant of the curves in $\mathcal{E}_{K,S}$. 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 $\mathcal{E}_{K,S}$.

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 $\mathfrak{p}$ 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 $\mathfrak{p}$. Then for any Weierstrass model of E, with invariants c_4, c_6, Δ, there exists an integer e such that*

$$\mathrm{ord}_{\mathfrak{p}}(\Delta) = 12e, \qquad \mathrm{ord}_{\mathfrak{p}}(c_4) \geq 4e, \qquad \mathrm{ord}_{\mathfrak{p}}(c_6) \geq 6e.$$

In addition, if $\mathrm{ord}_{\mathfrak{p}}(6) = 0$ then the above condition is sufficient.

Proof. See [CL07, Lemma 3.1]. □

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

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*

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

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 $(3u)^6 w \in K(S, 12)$. Then an elliptic curve E that Proposition 2.32 guarantees has the form

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

The idea of Cremona–Lingham method is to consider all possible[4] $w \in K(S, 6)_{12}$

[4]The set of w 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 $Ш(E/K)$ (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 λ using the relation of Theorem 2.5.

Chapter 3

Using λ–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 λ–invariants of the curves. If we know λ then by Theorem 2.5 we can compute j. However, λ is not a random element, instead λ 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 λ–invariant to compute $\mathcal{E}_{K,S}$ was suggested to John Cremona by Noam Elkies after a personal contact in July 2010.

Let $\mathfrak{p}$ 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 $\mathfrak{p}$ with discriminant Δ. 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

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

$$\Delta(g) = 2^4\Delta(f_{2,E}), \tag{3.2}$$

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

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

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 $\mathrm{Gal}(L/K) \simeq C_1$, 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 $\lambda, \mu \in \mathcal{O}^*_{L,S_L}$. We give necessary and sufficient conditions for λ and μ 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 λ–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 λ and μ often lie in subgroups of smaller rank than $\mathcal{O}^*_{L,S_L}$, 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 $S_z = \{\mathfrak{B} : \mathfrak{B} \text{ prime of } \mathcal{O}_{K_z}, \exists \mathfrak{p} \in S \text{ with } \mathfrak{B} \mid \mathfrak{p}\}$. We also denote $L_z = L(\zeta_3)$ and it holds $\mathrm{Gal}(L_z/K) = C_6$. Since $\gcd([K_z : K], [L_z : K_z]) = 1$, a prime $\mathfrak{p} \in S$ is ramified in L/K if and only if the primes in S_z above $\mathfrak{p}$ are ramified in L_z/K_z.

We construct L_z/K_z using the algorithm of the previous paragraph since $\zeta_3 \in K_z$ 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 $\mathrm{Gal}(L_z/K) = C_6$ 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

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

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

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 $N_{K_z/K}(a) \in K^{*3}$.*

Let $a\tau(a) = \beta^3$ where $\beta \in K^*$. Since $\zeta_3 \notin K$ we understand that β 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,

$$f(X) = X^3 - 3eX - e\,\mathrm{Tr}_{K_z/K}(\tilde{\beta}) = X^3 - 3\beta X - \mathrm{Tr}_{K_z/K}(a),$$

where $e = N_{K_z/K}(\tilde{\beta}) = \beta$ and $\mathrm{Tr}_{K_z/K}(\tilde{\beta}) = \frac{\mathrm{Tr}_{K_z/K}(a)}{\beta}$. 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 $D_p = S_3$.

Let $K \subset M \subset L$ be a tower of Galois extensions where $\mathrm{Gal}(M/K) \simeq C_2$ and[1] $\mathrm{Gal}(L/M) \simeq C_p$ where p is an odd prime $p \equiv 3 \mod 4$. We fix the notation such that $\mathrm{Gal}(L/M) = \langle\sigma\rangle$, $\mathrm{Gal}(M/K) = \langle\tau\rangle$, $f(x) \in M[x]$ 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^τ is the splitting field of f^τ . We use the same notation for any lift of τ and σ to the absolute Galois group $\mathrm{Gal}(\bar{K}/K)$.

Proposition 4.2. *It holds that L^τ/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. □

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 $\Leftrightarrow \forall \phi \in \mathrm{Gal}(\bar{K}/K) : \phi(L) = L \Leftrightarrow \sigma(L) = L$ and $\tau(L) = L \Leftrightarrow \tau(L) = L$ since L/M is Galois. □

From now on we assume that L/K is Galois. The group $\mathrm{Gal}(L/K)$ 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 $\mathrm{Gal}(K(h)/K) = C_p$ and as a result to distinguish[2] $\mathrm{Gal}(L/K) = D_p$ 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 $\Delta(f) \neq \square$ in K^* if and only if $\mathrm{Gal}(L/K) \simeq D_p$.*

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 $\Delta(f) = \square \Leftrightarrow \mathrm{Gal}(K(f)/K) = C_p \Leftrightarrow \mathrm{Gal}(L/K) = C_{2p}$. □

[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 $\mathrm{Gal}(L/K) = D_p$ we may assume that σ 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,

$$\begin{aligned} h(x) &= (x - a_1 - b_1)(x - a_2 - b_2)\cdots(x - a_p - b_p) \\ &= (x - a_1 - \sigma(a_1))(x - a_2 - \sigma(a_2))\cdots(x - a_p - \sigma(a_p)) \end{aligned} \tag{4.1}$$

with[3] $a_1 + b_1 \neq 0$. By the choice of the action of τ and σ 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 σ to δ 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 $(a_1 + b_1) + (a_2 + b_2) \cdots + (a_p + b_p) =$

[3] If $a_1 + b_1 = 0$ then $a_1 + b_2 \neq 0$ since $b_1 \neq b_2$. So we can change $h(x)$ 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. $\square$

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 $\tau \in \mathrm{Gal}(L/K)$ 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 $\mathrm{Gal}(L/K) \simeq D_p$.

(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 $\mathrm{Gal}(L/K) \simeq D_p$.

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 $d \in \{-1, \pm 2, \pm 3, \pm 23, \pm 6, \pm 46, \pm 69, \pm 138\}$.

Since $\zeta_3 \notin \mathbb{Q}$ we have to consider the case where we adjoin ζ_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.

field	discriminant
$x^3 - 138x - 644$	$-2^6 3^8 23^4$
$x^3 - x^2 + 8x - 6$	$-2^6 23^4$
$x^3 - 3x - 4$	$-2^6 3^8$
$x^3 + 69x - 230$	$-2^6 3^8 23^4$
$x^3 - x - 1$	-23^3
$x^3 - 23$	$-3^7 23^4$
$x^3 - 2$	$-2^4 3^7$
$x^3 - x^2 - 61x - 167$	$-2^4 3^3 23^4$
$x^3 - 92$	$-2^4 3^7 23^4$
$x^3 - 3$	-3^{11}
$x^3 - 207$	$-3^{11} 23^4$
$x^3 - 69$	$-3^{11} 23^4$
$x^3 - 18x - 30$	$-2^4 3^{11}$
$x^3 - 414$	$-2^4 3^{11} 23^4$
$x^3 - 276$	$-2^4 3^{11} 23^4$
$x^3 - 6$	$-2^4 3^{11}$
$x^3 - 828$	$-2^4 3^{11} 23^4$

$x^3 - 138$	$-2^4 3^{11} 23^4$
$x^3 - 18x - 6$	$2^4 3^{11} 23^3$
$x^3 - 6x - 3$	$3^7 23^3$
$x^3 - 54x - 150$	$2^4 3^{11} 23^3$
$x^3 - 36x - 78$	$2^4 3^{11} 23^3$
$x^3 - 6x - 20$	$-2^6 3^7 23^3$
$x^3 + 69x - 46$	$-2^9 3^8 23^4$
$x^3 - 3x - 10$	$-2^9 3^8$
$x^3 - x^2 - 15x - 29$	$-2^9 23^4$
$x^3 + 69x - 874$	$-2^9 3^8 23^4$
$x^3 - 93x - 346$	$-2^9 3^8 23^3$
$x^3 - 9x - 6$	$2^9 3^{11}$
$x^3 - x^2 + 8x + 40$	$-2^9 3^3 23^4$
$x^3 + 3x - 2$	$-2^9 3^7$
$x^3 + 69x - 322$	$-2^9 3^7 23^4$
$x^3 + 69x - 138$	$-2^9 3^7 23^4$
$x^3 - 9x - 42$	$-2^9 3^{11} 23^3$
$x^3 - 18x - 40$	$-2^9 3^7 23^3$
$x^3 + 63x - 66$	$-2^9 3^{11} 23^3$
$x^3 - 81x - 306$	$-2^9 3^{11} 23^3$

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 $\mathrm{Gal}(L/K) \subset S_3$ 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 = ∅.
4:     for a ∈ K(S, 2) and a ≠ 1 do
5:         Evaluate L = K(√a).
6:         Calculate the relative discriminant Δ(L/K).
7:         if ∃𝔭 ∉ S s.t. 𝔭 | Δ(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 $\zeta_3 \in K$

procedure CUBIC_INCLUDE_ZETA(K, S)
    Calculate $K(S,3)$.
    Fields $= \emptyset$.
    for $a \in K(S,3)$ and $a \neq 1$ **do**
        Evaluate $L = K(\sqrt[3]{a})$.
        Calculate the relative discriminant $\Delta(L/K)$.
        if $\exists \mathfrak{p} \notin S$ s.t. $\mathfrak{p} \mid \Delta(L/K)$ **then**
            L is not a solution.
        else
            Add L in Fields.
        end if
    end for
    return Fields.
end procedure

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

procedure CUBIC_NOT_INCLUDE_ZETA(K, S)
    Construct $K_z = K(\zeta_3)$.
    Calculate $S_z = \{\mathfrak{B} : \mathfrak{B}$ is a prime of $\mathcal{O}_{K_z}, \exists \mathfrak{p} \in S$ with $\mathfrak{B} \mid \mathfrak{p}\}$.
    Calculate $K_z(S_z, 3)$.
    Fields $= \emptyset$.
    for $a \in \ker\left(K_z(S_z,3) \xrightarrow{\text{Norm}} K(S,3)\right)$ and $a \neq 1$ **do**
        Find $\beta \in K^*$ s.t. $\beta^3 = N_{K_z/K}(a)$.
        Define $L = K(\theta)$, where θ is a root of $f(X) = X^3 - 3\beta X - Tr_{K_z/K}(a)$.
        Calculate the relative discriminant $\Delta(L/K)$.
        if $\exists \mathfrak{p} \notin S$ s.t. $\mathfrak{p} \mid \Delta(L/K)$ **then**
            L is not a solution.
        else
            Add L in Fields.
        end if
    end for
    return Fields.
end procedure

Algorithm 4 Cubic extensions unramified outside S

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

procedure S_3_EXTENSIONS(K, S)
  Fields $= \emptyset$.
  for M in QUADRATIC(K, S) **do**
    Evaluate $S_M = \{\mathfrak{B} : \mathfrak{B}$ prime of $\mathcal{O}_M, \exists \mathfrak{p} \in S$ with $\mathfrak{B} \mid \mathfrak{p}\}$.
    for L in CUBIC(M, S_M) **do**
      Let $f = x^3 - ax + b$ be a defining polynomial of L/M.
      if $f = f^\tau$ **then**
        Evaluate $\Delta(f)$.
        if $\Delta(f) \notin K^{*2}$ **then**
          Add L in Fields.
        end if
      else
        Let r_1 be a root of f and r_2 a root of f^τ.
        $r = r_1 + r_2$.
        if $r = 0$ **then**
          Replace r_2 with an other root of f^τ.
        end if
        Let h be the minimal polynomial of r over K.
        Evaluate $\Delta(h)$.
        if $\Delta(h) \notin K^{*2}$ **then**
          Add L in Fields.
        end if
      end if
    end for
  end for
  return Fields.
end procedure

Chapter 5

Solving S–unit equations

In this chapter we show that the solutions λ and μ 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 $\langle g_{0,1}, g_{1,1}, \cdots, g_{n,1} \rangle$ and $\langle g_{0,2}, g_{1,2}, \cdots, g_{m,2} \rangle$ 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

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

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 Ξ_0 of Ξ that can be used for practical computations. After computing Ξ_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 Ξ_0 for Ξ.
- Using lattice approximation reduction methods we reduce the upper bound Ξ_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 λ and μ 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 $\Delta(E_1) = 2^4 b^2(a^2 - 4b)$ and $\Delta(E_2) = 2^8 b(a^2 - 4b)^2$. 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 $\left(\frac{\cdot}{K}\right)$ 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 $(\frac{1}{4b}, \frac{1}{8(a^2-4b)}, a)$. □

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

$$\prod_{i=2}^{4} \Delta(E_i) \equiv -1 \mod K^{*2}, \qquad \left(\frac{\Delta(E_i), \Delta(E_j)}{K}\right) = 1$$

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 $\Delta(E_2) = 2^8 b(a^2 - 4b)^2 \equiv b = e_1 e_2 \mod K^{*2}$. Using a change of variables in E_1 we can show that $\Delta(E_3) \equiv e_1(e_1 - e_2) \mod K^{*2}$ and $\Delta(E_4) \equiv e_2(e_2 - e_1) \mod K^{*2}$. 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 $\Delta(E_2) = e_1 e_2 w_2^2$ 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 $\mathfrak{p}$ 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 $\mathfrak{p}$ be a prime of K above 2 not in S. Then*[1] $\mathrm{ord}_{\mathfrak{p}}(\Delta(L/K)) \equiv 0 \mod 2$.

[1] In case $[L : K] = 6$ we can prove that $\mathrm{ord}_{\mathfrak{p}}(\Delta(L/K)) \equiv 0 \mod 2 \Leftrightarrow \mathrm{ord}_{\mathfrak{p}}(\Delta(L_c/K)) \equiv 0 \mod 2$ where L_c is the cubic subfield of L/K.

Proof. Let Δ be the discriminant of E and $f_{2,E}$ its 2–division polynomial. By Proposition 2.31 we have that $\mathrm{ord}_{\mathfrak{p}}(\Delta) \equiv 0 \mod 2$. By equations (3.1)–(3.3) we obtain $(2^8\Delta)^t = k^2\Delta(L/K)$ for some $k \in K^*$. Thus, $\mathrm{ord}_{\mathfrak{p}}(\Delta(L/K)) \equiv 0 \mod 2$. □

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, λ is a λ–invariant of E, $\mu = 1-\lambda$, L is the 2–division field of E and $S_L = \{\mathfrak{B} \subset \mathcal{O}_L : \mathfrak{B} \text{ is a prime such that } \exists \mathfrak{p} \in S^{(2)} \text{ with } \mathfrak{B}|\mathfrak{p}\}$. The pair (λ, μ) is a solution of the S–unit equation

$$\lambda + \mu = 1 \tag{5.1}$$

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 $\mathrm{PGL}_2(\mathbb{Z})$ 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 $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{PGL}_2(\mathbb{Z})$.

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

2.5 we see that all the elements of Λ are distinct. We define

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

where T and R have order 2 and 3 respectively. Let $G := \langle T, S \rangle \simeq S_3$ then G acts on Λ as a permutation group on the roots of the polynomial $F_j(x) = \prod_{\lambda' \in \Lambda} (x - \lambda') = (x^2 - x + 1)^3 - \frac{j}{2^8} x^2 (1-x)^2 \in K[x]$. Because $L \supseteq K(\lambda)$ the splitting field of F_j is a subfield of L. From the above we understand that $\mathrm{Gal}(L/K)$ acts on Λ in the same way as a subgroup of G.

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

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

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

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

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

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

In the case $\mathrm{Gal}(L/K)$ 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 $\lambda, \mu \in \mathcal{O}_{K,S^{(2)}}$ or make use of Proposition 5.1.

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

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

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

Conversely, if $\mathrm{Norm}_{L/K}(\lambda) = 1$ that means $\tau(\lambda) = \frac{1}{\lambda}$ and then $\tau(j) = j$. Since, $\lambda, \mu \in \mathcal{O}^*_{L,S_L}$ we have that $v_{\mathfrak{B}}(\lambda^2 - \lambda + 1) \geq 0$ for all $\mathfrak{B} \notin S_L$ 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 μ does not satisfy extra conditions apart from the fact that $\mu \in \mathcal{O}^*_{L,S_L}$.

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

In this case the following theorem holds,

Theorem 5.6. *Let $\mathrm{Gal}(L/K) = \langle \sigma \rangle$. 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, μ *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 $\mathrm{Norm}_{L/K}(-\lambda) = 1$. The proof of the converse is similar to Theorem 5.5. □

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

5.3.4 $\mathrm{Gal}(L/K) \simeq S_3$

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

Theorem 5.7. *Let* $\mathrm{Gal}(L/K) \simeq S_3 = \langle \sigma, \tau \rangle$ *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) $\lambda \in \mathcal{O}^*_{L,L^\tau,S_L,1}$,

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

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

Conversely, let $\lambda \in \mathcal{O}^*_{L,S_L}$ *and* j, w, μ *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 $\mathrm{Norm}_{L/L^\sigma}(-\lambda) = 1$ and $\mathrm{Norm}_{L/L^\tau}(\lambda) = 1$. The proof of the converse is similar to Theorem 5.5 $\square$

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_λ and G_μ subgroups of $\mathcal{O}^*_{L,S_L}$ as follow,

Definition 5.8. *Let K, S, E, L, S_L, λ and μ as usual. We define*

- $G_\lambda = G_\mu = \mathcal{O}_{K,S^{(2)}}$ *if* $[L : K] = 1$,
- $G_\lambda = \mathcal{O}^*_{L,K,S_L,1}$ *and* $G_\mu = \mathcal{O}^*_{L,S_L}$ *if* $[L : K] = 2$,
- $G_\lambda = \mathcal{O}^*_{L,K,S_L,\pm 1}$ *and*[2] $G_\mu = \sigma(G_\lambda)$ *if* $[L : K] = 3$ *where* $\mathrm{Gal}(L/K) = \langle\sigma\rangle$,
- $G_\lambda = \mathcal{O}^*_{L,L^\tau,S_L,1} \bigcap \mathcal{O}^*_{L,L^\sigma,S_L,\pm 1}$ *and* $G_\mu = \sigma(G_\lambda)$ *where* $\mathrm{Gal}(L/K) \simeq S_3 = \langle\sigma, \tau\rangle$ *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 λ and μ in the C_3 and S_3 cases play an important role in the sieve.

[2] 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 $\left(\frac{-2,d}{\mathbb{Q}}\right) = 1$ 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[3] (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 $\mathbb{Q}(\sqrt{d})$

[3]The set $\{\pm 1, -2, -3, -6, -46, -69, -138\}$ is the complement of $\{2, 3, 6, \pm 23, 46, 69, 138\}$ in $\mathbb{Q}(S, 2)$.

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_λ and $\mathcal{O}^*_{L,S_L}$ according to Theorem 5.5. We recall that in this case $G_\mu = \mathcal{O}^*_{L,S_L}$.

field	$\text{rank}(G_\lambda)$	$\text{rank}(\mathcal{O}^*_{L,S_L})$
t^2+1	0	3
t^2-2	2	5
t^2-3	2	5
t^2-6	2	5
t^2+23	2	5
t^2-46	2	5
t^2-23	1	4
t^2-69	1	4
t^2-138	1	4

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 $\text{rank}(G_\lambda) = 2$ while $\text{rank}(\mathcal{O}^*_{L,S_L}) = 5$. 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 $\text{Gal}(L/\mathbb{Q}) = S_3$. Using Theorem 5.7 we have the following table for the rank of G_λ and $\mathcal{O}^*_{L,S_L}$. Again we recall that in this case $\text{rank}(G_\lambda) = \text{rank}(G_\mu)$ but $G_\lambda \neq G_\mu$.

field	$\mathrm{rank}(G_\lambda)$	$\mathrm{rank}(\mathcal{O}^*_{L,S_L})$
$x^3 - 138x - 644$	2	7
$x^3 - x^2 + 8x - 6$	3	9
$x^3 - 3x - 4$	3	9
$x^3 + 69x - 230$	2	7
$x^3 - x - 1$	2	9
$x^3 - 23$	2	7
$x^3 - 2$	2	7
$x^3 - x^2 - 61x - 167$	2	7
$x^3 - 92$	1	5
$x^3 - 3$	3	9
$x^3 - 207$	2	7
$x^3 - 69$	2	7
$x^3 - 18x - 30$	2	7
$x^3 - 414$	1	5
$x^3 - 276$	1	5
$x^3 - 6$	2	7
$x^3 - 828$	1	5
$x^3 - 138$	1	5
$x^3 - 18x - 6$	3	10
$x^3 - 6x - 3$	4	12
$x^3 - 54x - 150$	3	10
$x^3 - 36x - 78$	3	10

$x^3 - 6x - 20$	3	9
$x^3 + 69x - 46$	2	8
$x^3 - 3x - 10$	3	10
$x^3 - x^2 - 15x - 29$	2	8
$x^3 + 69x - 874$	2	8
$x^3 - 93x - 346$	3	9
$x^3 - 9x - 6$	3	11
$x^3 - x^2 + 8x + 40$	3	9
$x^3 + 3x - 2$	3	9
$x^3 + 69x - 322$	2	7
$x^3 + 69x - 138$	2	7
$x^3 - 9x - 42$	3	9
$x^3 - 18x - 40$	3	9
$x^3 + 63x - 66$	3	9
$x^3 - 81x - 306$	3	9

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 $\langle g_{0,1}, g_{1,1}, \cdots, g_{n,1} \rangle$ and $\langle g_{0,2}, g_{1,2}, \cdots, g_{m,2} \rangle$ 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

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

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 Ξ_0 of Ξ that can be used for practical computations. After computing Ξ_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 Ξ_0 for Ξ.

- Using lattice approximation reduction methods we reduce the upper bound Ξ_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 λ, μ and are related to the λ–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 λ and μ may lie in different subgroups of $\mathcal{O}^*_{L,S_L}$, we denote by G_λ and G_μ the subgroups of $\mathcal{O}^*_{L,S_L}$ where λ and μ 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 λ_0 and μ_0 are generators of the torsion part and λ_i, μ_j are bases for the free parts. For the rest of the chapter we fix bases for G_λ and G_μ and we express λ and μ as a multiplicative combination of the bases,

$$\lambda = \prod_{i=0}^{n} \lambda_i^{x_i} \qquad\qquad \mu = \prod_{j=0}^{m} \mu_j^{y_j}.$$

In the C_3 and S_3 cases where $\sigma(\lambda) = \frac{1}{\mu}$ we can make a choice of bases for G_λ and G_μ such that λ and μ have the same vector exponents, i.e. $n = m$ and $x_i = y_i$ for $i = 0, \cdots, n$. 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 choice bases for G_λ and G_μ such that some of the generators of the bases lie in $\mathcal{O}_K^*$.

Let M_L be the the set of places[1] of L then we define,

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

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

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_λ, S_μ do not contain prime ideals $\mathfrak{B}$ which are above non split primes of K. This holds because G_λ, G_μ 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_λ and S_μ and the second set contains the solutions with high absolute value at one or more places in S_λ or S_μ. Then we repeat this procedure until we find all the solutions.

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

[1]Both finite and infinite places.

For a fixed subset I of $\{0, 1, \cdots, n\}$ we define

$$S_I = \{\mathfrak{B} \in S_\lambda : \exists \lambda_i \text{ with } i \in I \text{ such that } |\lambda_i|_{\mathfrak{B}} \neq 1\}$$
$$\lambda_I = \prod_{i \in I} \lambda_i^{x_i}.$$

We denote by $I^\infty = \{i \in \{0, 1, \cdots, n\} : \lambda_i \in \mathcal{O}_K^*\}$, $S_\lambda^\infty = S_{I^\infty}$ and $\lambda_\infty := \lambda_{I^\infty}$. Similarly, we define S_J for a fixed subset J of $\{0, 1, \cdots, m\}$, μ_J, J^∞, S_μ^∞ and μ_∞.

6.1 Trivial solutions for $|x - 1|_{\mathfrak{p}} \ll 1$

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

$$|g - 1|_{\mathfrak{p}} \leq \delta \ll 1 \tag{6.3}$$

with $g \in G$, $\mathfrak{p}$ 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 $\mathfrak{p}$ 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 $|g-1|_{\mathfrak{p}} \leq \delta$ it holds,

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

Since δ is small then δ' 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]

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

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

Lemma 6.1. *Let*

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

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

Proof. Let

$$\Phi = \sum_{i=1}^{n} x_i [C\log|g_i|_{\mathfrak{p}}].$$

[2]We assume that $|g_n|_{\mathfrak{p}} \neq 1$.

Then

$$\left|\Phi - C\left(\sum_{i=1}^{n} x_i \log|g_i|_{\mathfrak{p}}\right)\right| \leq \frac{\sum_{i=1}^{n} b_i}{2}.$$

Thus

$$|\Phi| \leq |\Phi - C\log|g|_{\mathfrak{p}}| + |C\log|g|_{\mathfrak{p}}| \leq \frac{\sum_{i=1}^{n} b_i}{2} + C\delta'.$$

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 $\mathfrak{p}$ be a prime ideal of the number field K. Let p be the rational prime below $\mathfrak{p}$ and $e_{\mathfrak{p}}$ and $f_{\mathfrak{p}}$ the ramification and residual degree of $\mathfrak{p}$. We assume that

$$\delta' = -\frac{\log\delta}{e_{\mathfrak{p}} f_{\mathfrak{p}} \log p} \geq 1$$

which is not a very restricted condition since δ is very small in practice.

In the following lines we will show the p–adic analogue of Lemma 6.1. Since

$|g-1|_{\mathfrak{p}} \leq \delta < 1$ we have that $\mathrm{ord}_{\mathfrak{p}}(g) = 0$. By Lemma 2.16 we can find a finite set of elements $h_0, h_1, h_2, \cdots, h_t \in K^*$ such that

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

where $\mathrm{ord}_{\mathfrak{p}}(h_i) = 0$ for $i = 0, \cdots, t$ and $|y_i| \leq |x_i| \leq b_i$ for $i = 1, \cdots, t$.

Then we set

$$\Theta := \log_p(g) = \log_p(h_0) + \sum_{i=1}^{t} y_i \log_p(h_i) \in K_{\mathfrak{p}}.$$

Since $\delta' \geq 1$ and Section 2.3,

$$\mathrm{ord}_p(\Theta) = \mathrm{ord}_p(\log_p(g)) = \mathrm{ord}_p(g-1) \geq -\frac{\log \delta}{e_{\mathfrak{p}} f_{\mathfrak{p}} \log p} = \delta'.$$

Let $d = e_{\mathfrak{p}} f_{\mathfrak{p}} = [K_{\mathfrak{p}} : \mathbb{Q}_p]$ and $K_{\mathfrak{p}} = \mathbb{Q}_p(\phi)$. 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 $i = 0, \cdots, d-1$. As in [TW92, page 257] we can show that

$$\mathrm{ord}_p(\Theta_i) \geq \delta' - \frac{\mathrm{ord}_p(D(\phi))}{2} =: c_1$$

where $D(\phi) = \mathrm{disc}_{K_{\mathfrak{p}}/\mathbb{Q}_p}(1, \phi, \cdots, \phi^{d-1})$. We choose $\xi \in \mathbb{Q}_p$ such that

$$\mathrm{ord}_p(\xi) = \min_{0 \leq j \leq t} \left(\min_{0 \leq i \leq d-1} (\mathrm{ord}_p(\nu_{j,i})) \right) =: c_2$$

Dividing Θ_i by ξ we get

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

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

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

Since $c_1 = \delta' - \frac{\mathrm{ord}_p(D(\phi))}{2}$ and δ' 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

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

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 ℓ_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 $\mathrm{ord}_p(\frac{\Theta_i}{\xi}) \geq c_3 \geq u$ we have that

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

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

6.2 Decomposing the solutions

In this section we show how we can decompose the pairs (λ, μ) 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 $\mathrm{Gal}(L/K)$.

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

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

6.2.1 Quadratic extensions

Let τ be the generator of $\mathrm{Gal}(L/K)$. By Theorem 5.5 we can assume that we are looking for pairs of solutions (λ, μ) such that $\tau(\lambda) = \frac{1}{\lambda}$. Moreover, we have mentioned earlier that S_λ contains prime ideals $\mathfrak{B}$ above split primes of K and by Definition 5.8 we recall that $G_\mu = \mathcal{O}^*_{L,S_L}$. In addition $\mathrm{ord}_{\mathfrak{B}}(\lambda) = -\mathrm{ord}_{\tau(\mathfrak{B})}(\lambda)$ 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 (λ, μ) such that $|\mathrm{ord}_{\mathfrak{B}}(\lambda)|$ 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 δ. We do the same for $\mathfrak{B} \in S_\mu$ and λ instead of μ in order to prove that there do not exist pairs (λ, μ) such that $|\mathrm{ord}_{\mathfrak{B}}(\mu)|$ is 'large'. We use the new upper bounds on $|\mathrm{ord}_{\mathfrak{B}}(\lambda)|$ and $|\mathrm{ord}_{\mathfrak{B}}(\mu)|$ for the prime ideals of S_λ and S_μ respectively to get new vectors $B_1 = \left(b_0^{(1)}, b_1^{(1)}, \cdots, b_n^{(1)}\right)$ and $C_1 = \left(c_0^{(1)}, c_1^{(1)}, \cdots, c_m^{(1)}\right)$ such that $|x_i| \leq b_i^{(1)}$ and $|y_j| \leq c_j^{(1)}$ for $i = 0, 1, \cdots, n$ and $j = 0, 1, \cdots, m$.

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 $\mathfrak{B} \in S_\lambda^\infty \Leftrightarrow \tau(\mathfrak{B}) \in S_\lambda^\infty$.

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

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

Let

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

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

Proof. For a $\mathfrak{B} \in S_\lambda^\infty$ we have,

$$\begin{aligned}|\log|\lambda|_{\mathfrak{B}}| &\leq \sum_{i=0}^{n} |x_i||\log|\lambda_i|_{\mathfrak{B}}| \leq \sum_{i=0}^{n} b_i^{(1)} |\log|\lambda_i|_{\mathfrak{B}}| \\ &\leq \max_{\mathfrak{B}\in S_\lambda^\infty} \left(\sum_{i=0}^{n} b_i^{(1)} |\log|\lambda_i|_{\mathfrak{B}}|\right) = \log(R_{1,\infty}).\end{aligned}$$

□

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 $\mathfrak{B} \in S_\lambda^\infty$ and $1 < R' < R$ we define,*

$$\mathcal{T}^2_{\mathfrak{B}}(B, C, R, R') = \left\{(\lambda, \mu) \in \mathcal{L}^2_\infty(B, C, R) : |\mu - 1|_{\mathfrak{B}} < \frac{1}{R'}\right\}.$$

We need the following lemma.

Lemma 6.6. *There exists a computable constant $c_{1,\infty} > 0$ such that*

$$|x_i| \leq c_{1,\infty} \max_{\mathfrak{B}\in S_\lambda^\infty} \left(|\log|\lambda_\infty|_{\mathfrak{B}}|\right),$$

for all $i \in I^\infty$.

Proof. We can assume that $I^\infty = \{1, 2, \cdots, t\}$ and $S_\lambda^\infty = \{\mathfrak{B}_1, \mathfrak{B}_2, \cdots, \mathfrak{B}_u\}$ with

$t \leq u$. We define the matrix

$$M = \begin{pmatrix} \log|\lambda_1|_{\mathfrak{B}_1} & \cdots & \log|\lambda_t|_{\mathfrak{B}_1} \\ \vdots & & \vdots \\ \log|\lambda_1|_{\mathfrak{B}_u} & \cdots & \log|\lambda_t|_{\mathfrak{B}_u} \end{pmatrix}$$

By the choice of I^∞ and S_λ^∞ 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 $|x_i| \leq c_{1,\infty} \max_{\mathfrak{B} \in S_\lambda^\infty} (|\log|\lambda_\infty|_{\mathfrak{B}}|)$ for all $i \in I^\infty$. □

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

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

$$\mathcal{L}^2_\infty(B_k, C_k, R_k) = \mathcal{L}^2_\infty(B_{k+1}, C_{k+1}, R_{k+1}) \cup \bigcup_{\mathfrak{B} \in S_\lambda^\infty} \mathcal{T}^2_{\mathfrak{B}}(B_k, C_k, R_k, R_{k+1})$$

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* $c_{2,\infty} = \max_{\mathfrak{B} \in S_\lambda^\infty} \left(\sum_{i \notin I^\infty} b_i^{(k)} |\log|\lambda_i|_{\mathfrak{B}}|\right)$.

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

$$|\lambda|_{\mathfrak{B}} > R_{k+1} \Leftrightarrow |\tau(\lambda)|_{\tau(\mathfrak{B})} > R_{k+1} \Leftrightarrow$$
$$|\lambda|_{\tau(\mathfrak{B})} < \frac{1}{R_{k+1}} \Leftrightarrow |\mu - 1|_{\tau(\mathfrak{B})} < \frac{1}{R_{k+1}}.$$

In the second case we have

$$|\lambda|_{\mathfrak{B}} < \frac{1}{R_{k+1}} \Leftrightarrow |\mu - 1|_{\mathfrak{B}} < \frac{1}{R_{k+1}}.$$

We have shown that

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

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

$$|\log|\lambda_{\infty}|_{\mathfrak{B}}| \leq |\log|\lambda|_{\mathfrak{B}}| + |\log|\frac{\lambda}{\lambda_{\infty}}|_{\mathfrak{B}}| < \log R_{k+1} + c_{2,\infty}.$$

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 $(\lambda, \mu) \in \mathcal{L}^2_{\infty}(B_{k+1}, C_{k+1}, R_{k+1})$. □

Proposition 6.7 is very useful in practice because proving that the sets $\mathcal{T}^2_{\mathfrak{B}}(B_k, C_k, R_k, R_{k+1})$ 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 $|\operatorname{ord}_{\mathfrak{B}}(\lambda)|$ for $\mathfrak{B} \notin S^{\infty}_{\lambda}$, $c_{2,\infty}$ is small.

6.2.2 Cubic extensions

Let σ be a generator of $\mathrm{Gal}(L/K)$. By Theorem 5.6 we can assume that we are looking for pairs of solutions (λ, μ) such that $\sigma(\lambda) = \frac{1}{\mu}$. Moreover, we have made a choice of G_λ and G_μ such that λ and μ 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 λ 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_λ and S_μ 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 (λ, μ) such that $|\operatorname{ord}_{\mathfrak{B}}(\lambda)|$ 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 δ. We use the new upper bounds on $|\operatorname{ord}_{\mathfrak{B}}(\lambda)|$ for all prime ideals of S_λ to get a new vector $B_1 = \left(b_0^{(1)}, b_1^{(1)}, \cdots, b_n^{(1)}\right)$ 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,*

$$\mathcal{L}_\infty^3(B, R) = \{(\lambda, \mu) : |x_i| \leq b_i, |\log |\lambda|_{\mathfrak{B}}| \leq \log R, \forall \mathfrak{B} \in S_\lambda^\infty\}$$

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

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

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* $\mathfrak{B} \in S_\lambda^\infty$ *and* $1 < R' < R$ *we define,*

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

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,*

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

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

Proof. The proof is similar to Proposition 6.7. □

6.2.3 S_3 extensions

Let σ and τ be the generator of $\mathrm{Gal}(L/K)$ 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 (λ, μ) such that $\tau(\lambda) = \frac{1}{\lambda}$ and $\sigma(\lambda) = \frac{1}{\mu}$. Moreover, we have made a choice of G_λ and G_μ such that λ and μ 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 $\mu_i = \sigma(\frac{1}{\lambda_i})$ and so it is enough to consider only the bound vector for λ. So we understand that $G_\mu = \sigma(G_\lambda)$ and $I^\infty = J^\infty$.

As we mentioned earlier S_λ and S_μ contain only prime ideals $\mathfrak{B}$ above split primes of K. Again, the first step is to find an upper bound of $|\operatorname{ord}_{\mathfrak{B}}(\lambda)|$ 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 δ. We use the new upper bounds on $|\operatorname{ord}_{\mathfrak{B}}(\lambda)|$ for all prime ideals of S_λ to get a new vector $B_1 = \left(b_0^{(1)}, b_1^{(1)}, \cdots, b_n^{(1)}\right)$ such that $|x_i| \leq b_i^{(1)}$ for $i = 0, 1, \cdots, n$.

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

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

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

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

Proof. The proof is similar to Lemma 6.4. □

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

$$\mathcal{T}_{\mathfrak{B}}^6(B, R, R') = \left\{ (\lambda, \mu) \in \mathcal{L}_\infty^6(B, R) : \begin{array}{c} |\mu - 1|_{\mathfrak{B}} < \frac{1}{R'} \text{ or} \\ |\lambda - 1|_{\mathfrak{B}} < \frac{1}{R'} \text{ or} \\ |\mu - 1|_{\sigma^2(\mathfrak{B})} < \frac{1}{R'} \text{ or} \\ |\lambda - 1|_{\sigma(\mathfrak{B})} < \frac{1}{R'} \end{array} \right\}.$$

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

Proposition 6.15. *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,*

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

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

Proof. The proof is similar to Proposition 6.7. □

We should mention that in this case it may happen that there exists $\mathfrak{B} \in S_\lambda^\infty \cup S_\mu^\infty$ 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 λ 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 $\mathcal{T}_{\mathfrak{B}}^i$ 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 $\mathcal{T}_{\mathfrak{B}}^{i}$ do not contain non–trivial elements then we have to start computing solutions. The first step is to find congruence solutions mod $\mathfrak{B}^e$ of μ and λ for suitable choices of finite primes $\mathfrak{B}$ 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 ([FP85]), as Smart and Wildanger do, to determine which lifts of the mod $\mathfrak{B}^e$ 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 (λ, μ) 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_μ. For a fixed prime ideal $\mathfrak{B} \in S_\lambda$ we define

$$b_\lambda = b_\lambda(\mathfrak{B}) = \max_{\lambda \in W_\lambda} \{|\operatorname{ord}_{\mathfrak{B}}(\lambda)|\} \qquad b_\mu = b_\mu(\mathfrak{B}) = \max_{\mu \in W_\mu} \{|\operatorname{ord}_{\mathfrak{B}}(\mu)|\}.$$

6.3.1 Quadratic case

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

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

Proof. We have to consider three cases.

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

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

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

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

□

Proposition 6.16 says that reducing b_μ and $\overline{b}_\mu$ we reduce b_λ too. We will show how we can find new smaller b_μ and $\overline{b}_\mu$ by computing solutions in congruence equations. For here and later on we focus only on $\mathfrak{B}$ and b_μ. 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 $R = p^{f_{\mathfrak{B}} e}$, 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_μ. We want to determine all pairs $(\lambda, \mu) \in W$ such that $|\operatorname{ord}_{\mathfrak{B}}(\mu)| \geq e > 0$. In the case $\operatorname{ord}_{\mathfrak{B}}(\mu) > 0$ we find λ using the fact that

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

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

$$|\mu|_{\mathfrak{B}} \geq R \Leftrightarrow \left|\frac{1}{\mu}\right|_{\mathfrak{B}} \leq \frac{1}{R} \Leftrightarrow \left|\frac{1}{1-\lambda}\right|_{\mathfrak{B}} \leq \frac{1}{R} \Leftrightarrow$$
$$\left|1 + \frac{\lambda}{1-\lambda}\right|_{\mathfrak{B}} \leq \frac{1}{R} \Leftrightarrow 1 \equiv \frac{\lambda}{\lambda - 1} \mod \mathfrak{B}^e$$

We just showed the following proposition.

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

In practice we find the solutions for $x \equiv 1 \mod \mathfrak{B}^e$ and then we check if x corresponds to an element $\overline{x}$ of $\mathcal{O}^*_{L,S_L}$ that satisfies $1 - \overline{x} \in \mathcal{O}^*_{L,S_L}$. 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_λ and G_μ such that $\mu_i = \sigma(\frac{1}{\lambda_i})$ for $i = 0, 1, \cdots, n$ where σ is a generator of $\operatorname{Gal}(L/K)$. Let $(\lambda, \mu) \in W$ for which we recall that $\sigma(\lambda) = \frac{1}{\mu}$. We fix a prime ideal $\mathfrak{B} \in S_\lambda$.

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

Proof. Let (λ, μ) be a pair such that $|\operatorname{ord}_{\mathfrak{B}}(\lambda)| > b_\mu$. We know that either $\operatorname{ord}_{\mathfrak{B}}(\lambda) = \operatorname{ord}_{\mathfrak{B}}(\mu) < -b_\mu$ or $\operatorname{ord}_{\mathfrak{B}}(\lambda) > b_\mu$ and $\operatorname{ord}_{\mathfrak{B}}(\mu) = 0$. In the first case we understand that $|\operatorname{ord}_{\mathfrak{B}}(\mu)| > b_\mu$ 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 $|\operatorname{ord}_{\mathfrak{B}}(-\frac{\mu}{\lambda})| = |\operatorname{ord}_{\mathfrak{B}}(\lambda)| > b_\mu$ which is a contradiction. So $b_\lambda \leq b_\mu$. By symmetry we have $b_\mu \leq b_\lambda$. □

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

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

Proof. Let $R = p^{ef_{\mathfrak{B}}}$ where p is the rational prime below $\mathfrak{B}$ and $f_{\mathfrak{B}}$ the residual degree of $\mathfrak{B}$. We have that $|\operatorname{ord}_{\mathfrak{B}}(\mu)| \geq e \Leftrightarrow |\log|\mu|_{\mathfrak{B}}| \geq \log R$. Taking into account that $\sigma(\lambda) = \frac{1}{\mu}$ and $\sigma(\mu) = \frac{-\lambda}{1-\lambda}$ we have that

- $\log|\mu|_{\mathfrak{B}} \geq \log R \Leftrightarrow \left|\frac{1}{\mu}\right|_{\mathfrak{B}} \leq \frac{1}{R} \Leftrightarrow \left|\frac{1}{\lambda} - 1\right|_{\sigma(\mathfrak{B})} \leq \frac{1}{R}$.
- $\log|\mu|_{\mathfrak{B}} \leq -\log R \Leftrightarrow |\mu|_{\mathfrak{B}} \leq \frac{1}{R} \Leftrightarrow |\lambda - 1|_{\mathfrak{B}} \leq \frac{1}{R}$.

□

We recall that $S_\lambda = S_\mu$ contains primes $\mathfrak{B}$ which are above primes $\mathfrak{p}$ of K that split. Let $\mathfrak{B}_1, \mathfrak{B}_2, \mathfrak{B}_3$ be three conjugate prime ideals of L such that $\sigma(\mathfrak{B}_i) = \mathfrak{B}_{i+1}$ for $i = 1, 2$ and $\sigma(\mathfrak{B}_3) = \mathfrak{B}_1$. By Theorem 5.6 we have that

$$\sum_{i=1}^{3} \operatorname{ord}_{\mathfrak{B}_i}(\lambda) = \sum_{i=1}^{3} \operatorname{ord}_{\mathfrak{B}_i}(\mu) = 0.$$

Let $a_1 = \mathrm{ord}_{\mathfrak{B}_1}(\lambda)$ and $a_2 = \mathrm{ord}_{\mathfrak{B}_2}(\lambda)$. By the above relation and the fact that $\sigma(\lambda) = \frac{1}{\mu}$ we have

$$a_1 = \mathrm{ord}_{\mathfrak{B}_1}(\lambda) \qquad a_1 + a_2 = \mathrm{ord}_{\mathfrak{B}_1}(\mu) \tag{6.4}$$

$$a_2 = \mathrm{ord}_{\mathfrak{B}_2}(\lambda) \qquad -a_1 = \mathrm{ord}_{\mathfrak{B}_2}(\mu) \tag{6.5}$$

$$-a_1 - a_2 = \mathrm{ord}_{\mathfrak{B}_3}(\lambda) \qquad -a_2 = \mathrm{ord}_{\mathfrak{B}_3}(\mu) \tag{6.6}$$

Proposition 6.20. *$b_\lambda(\mathfrak{B}_i) = b_\mu(\mathfrak{B}_j)$ for $i, j = 1, 2, 3$.*

Proof. By Proposition 6.18 it is enough to show that $b_\lambda(\mathfrak{B}_1) = b_\lambda(\mathfrak{B}_2)$. Assume that there exists a pair $(\lambda, \mu) \in W$ such that $|\mathrm{ord}_{\mathfrak{B}_1}(\lambda)| > b_\lambda(\mathfrak{B}_2)$. We have to consider two cases.

- Suppose that $\mathrm{ord}_{\mathfrak{B}_1}(\lambda) > b_\lambda(\mathfrak{B}_2)$. Then by equations (6.4)–(6.6) we understand that $a_1 > 0$ and $a_2 = -a_1$. So, we see $|\mathrm{ord}_{\mathfrak{B}_1}(\lambda)| = |\mathrm{ord}_{\mathfrak{B}_2}(\lambda)| \leq b_\lambda(\mathfrak{B}_2)$.

- Suppose that $\mathrm{ord}_{\mathfrak{B}_1}(\lambda) < -b_\lambda(\mathfrak{B}_2)$. Again by equations (6.4)–(6.6) we conclude that $a_1 < 0$ and $a_2 = 0$. As a result we understand that $|\mathrm{ord}_{\mathfrak{B}_1}(\lambda)| = |\mathrm{ord}_{\mathfrak{B}_2}(\mu)| \leq b_\mu(\mathfrak{B}_2) = b_\lambda(\mathfrak{B}_2)$ by Proposition 6.18.

□

Propositions 6.18, 6.19 and 6.20 say that it is enough to find the solutions of $x \equiv 1 \mod \mathfrak{B}_1^e$ and $x \equiv 1 \mod \mathfrak{B}_2^e$ and check which lifts $\overline{x} \in G_\lambda$ satisfy $1 - \overline{x} \in \mathcal{O}^*_{L,S_L}$.

6.3.3 S_3 case

Let $\mathrm{Gal}(L/K) = \langle \sigma, \tau \rangle$ such that $\sigma^3 = \tau^2 = 1$ and $\tau\sigma\tau = \sigma^{-1}$. We recall that we have chosen bases for G_λ and G_μ such that $\mu_i = \sigma(\frac{1}{\lambda_i})$ for $i = 0, 1, \cdots, n$. Let (λ, μ) 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_λ and S_μ contain prime ideals $\mathfrak{B}$ of L which are above primes $\mathfrak{p}$ of K that split. Let $g_\mathfrak{B}$ be the number of conjugate prime ideals of $\mathfrak{B}$.

Proposition 6.21. *S_λ and S_μ 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_λ and S_μ 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 $\mathrm{Norm}_{L/L^\sigma}(\lambda) = \lambda\sigma(\lambda)\sigma^2(\lambda) = -1$. Since $g_\mathfrak{B} = 2$ we have that the decomposition group $D_\mathfrak{B}(L/K) = \langle \sigma \rangle$. That shows $\mathrm{ord}_\mathfrak{B}(\lambda) = 0$. Similarly for S_μ. □

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 $\mathfrak{B}_3 \notin S_\lambda$ such that $\mathrm{ord}_{\mathfrak{B}_1}(\lambda) = -\mathrm{ord}_{\mathfrak{B}_2}(\lambda)$. Similarly, $\mathfrak{B}_2, \mathfrak{B}_3 \in S_\mu$ and $\mathfrak{B}_1 \notin S_\mu$ such that $\mathrm{ord}_{\mathfrak{B}_2}(\mu) = -\mathrm{ord}_{\mathfrak{B}_3}(\mu)$.

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*

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

Proof. The relation

$$-\operatorname{ord}_{\mathfrak{B}_1}(\lambda) = \operatorname{ord}_{\mathfrak{B}_2}(\lambda) = -\operatorname{ord}_{\mathfrak{B}_3}(\mu) = \operatorname{ord}_{\mathfrak{B}_2}(\mu) \leq 0,$$

is an immediate consequence of the analysis in the paragraph above the proposition. As a results 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 $x \equiv 1 \mod \mathfrak{B}_3^e$ and check which lifts $\overline{x} \in G_\lambda$ satisfy $1 - \overline{x} \in \mathcal{O}_{L,S_L}^*$.

Case $g_{\mathfrak{B}} = 6$. 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

$$a_1 = \operatorname{ord}_{\mathfrak{B}_1}(\lambda) = -\operatorname{ord}_{\mathfrak{B}_2}(\lambda) = -\operatorname{ord}_{\mathfrak{B}_3}(\mu) = \operatorname{ord}_{\mathfrak{B}_4}(\mu) \tag{6.7}$$

$$-a_1 - a_2 = \operatorname{ord}_{\mathfrak{B}_3}(\lambda) = -\operatorname{ord}_{\mathfrak{B}_6}(\lambda) = -\operatorname{ord}_{\mathfrak{B}_5}(\mu) = \operatorname{ord}_{\mathfrak{B}_2}(\mu) \tag{6.8}$$

$$a_2 = \operatorname{ord}_{\mathfrak{B}_5}(\lambda) = -\operatorname{ord}_{\mathfrak{B}_4}(\lambda) = -\operatorname{ord}_{\mathfrak{B}_1}(\mu) = \operatorname{ord}_{\mathfrak{B}_6}(\mu) \tag{6.9}$$

Proposition 6.23.

$$b_\lambda(\mathfrak{B}_i) = b_\lambda(\tau(\mathfrak{B}_i))$$

$$b_\mu(\mathfrak{B}_i) = b_\mu(\sigma^2\tau(\mathfrak{B}_i))$$

$$b_\lambda(\mathfrak{B}_i) = b_\mu(\sigma(\mathfrak{B}_i))$$

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* $|\operatorname{ord}_{\mathfrak{B}}(\mu)| \geq e > 0$. *Then either* $\lambda \equiv 1 \mod \mathfrak{B}^e$ *or* $\frac{1}{\lambda} \equiv 1 \mod (\sigma(\mathfrak{B}))^e$.

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 $x \equiv 1 \mod \mathfrak{B}_i^e$ for $i = 1, 3, 5$(or $2, 4, 6$) and test which lifts $\overline{x} \in G_\lambda$ satisfy $1 - \overline{x} \in \mathcal{O}_{L,S_L}^*$.

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

For a fixed λ_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 $\lambda_0 \prod_{i=1}^n \lambda_i^{x_i} \equiv 1 \mod \mathfrak{B}^e$ or $1 \equiv \frac{\lambda_0 \prod_{i=1}^n \lambda_i^{x_i}}{\lambda_0 \prod_{i=1}^n \lambda_i^{x_i} - 1} \mod \mathfrak{B}^e$. 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

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

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

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

where p is the rational prime below $\mathfrak{Q}$ and $f_{\mathfrak{Q}}$ the residual degree. Let $\mathfrak{Q}_1, \cdots, \mathfrak{Q}_f$ be the elements of S_λ. We consider the matrix

$$A = \begin{pmatrix} \frac{\log|\lambda_{1,k}|_{\mathfrak{Q}_1}}{\log(r_{\mathfrak{Q}_1})} & \cdots & \frac{\log|\lambda_{n,k}|_{\mathfrak{Q}_1}}{\log(r_{\mathfrak{Q}_1})} \\ \vdots & & \vdots \\ \frac{\log|\lambda_{1,k}|_{\mathfrak{Q}_f}}{\log(r_{\mathfrak{Q}_f})} & \cdots & \frac{\log|\lambda_{n,k}|_{\mathfrak{Q}_f}}{\log(r_{\mathfrak{Q}_f})} \end{pmatrix} \in \mathbb{R}^{f \times n},$$

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

$$\|A\vec{t}\|^2 \leq f.$$

Proof. We have that $|\log|\lambda|_{\mathfrak{Q}}| \leq \log R$ for all $\mathfrak{Q} \in S_\lambda^\infty$. We know that $\lambda =$

$\rho \prod_{i=1}^{n} \lambda_{i,k}^{t_i}$ for some $\rho \in \Lambda_{0,\mathrm{con}}$. Then it holds

$$\left|\log|\prod_{i=1}^{n} \lambda_{i,k}^{t_i}|_{\mathfrak{Q}}\right| = \left|\log|\lambda\rho^{-1}|_{\mathfrak{Q}}\right| \leq |\log|\lambda|_{\mathfrak{Q}}| + |\log|\rho|_{\mathfrak{Q}}|$$
$$\leq \log R + |\log|\rho|_{\mathfrak{Q}}| \leq \log r_{\mathfrak{Q}}.$$

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

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

□

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

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 $x \equiv 1 \mod \mathfrak{B}^e$ 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 (λ, μ)

always satisfy $\left(\frac{\lambda,\mu}{\mathfrak{B}}\right)_\ell$ for every prime $\mathfrak{B}$ and integer $\ell \geq 1$. For a suitable choice[4] of $\mathfrak{B}$ and ℓ we create the matrix $A_{\mathfrak{B}} = \left(\left(\frac{\lambda_i,\mu_j}{\mathfrak{B}}\right)_\ell\right)_{i,j} \in \mathbb{M}_{n+1,n+1}(\mathbb{Z}/\ell\mathbb{Z})$ 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 $1 - x \in \mathcal{O}_{K,S}^*$. We assume for $\mathfrak{p} \in S$ that S contains all the conjugate of $\mathfrak{p}$. We define $S_{\mathbb{Q}} = \{p \in \mathbb{Z} : \exists \mathfrak{p} \in S, \mathfrak{p}|p\}$.

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 $f_x(1) \in \mathbb{Z}_{S_{\mathbb{Q}}}^*$ if and only if $1 - x \in \mathcal{O}_{K,S}^*$.*

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 $f_x(t) = \det(It - A_x)$ 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. □

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 $\mathcal{O}_{K,S}^*$ ([Dev16]).

[4]We use *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 $S_\lambda \cup S_\mu$ and ℓ 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 λ–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 λ–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_λ is the maximal among all the 9 fields. We have that

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

Since 23 is the only prime in S which splits in L we have that S_λ contains only the two primes $\mathfrak{B}_1$ and $\mathfrak{B}_2$ above 23. On the other hand S_μ contains all the primes in L above S since $G_\mu = \mathcal{O}^*_{L,S_L}$ 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_λ and G_μ. 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_μ 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 λ is not so big, just 6005 elements, and we can compute them with a simple loop. At the end we have that

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

From this set of W_λ we have the candidate set of j–invariants

$$\begin{aligned} \Big\{ & \frac{3065617154}{9}, \frac{545138290809}{16928}, \frac{135638288072}{42849}, 287496, \frac{135559106353}{5037138}, \\ & \frac{148877000}{4761}, 8000, \frac{2315250}{529}, \frac{2744000}{9}, 10976, \frac{13144256}{4761}, \frac{953312}{529}, \\ & \frac{115387499277504}{148035889}, \frac{870436774592}{204004089}, 1728 \Big\} \end{aligned}$$

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

$\mathbb{Q}$ which have a rational point of order 2 and good reduction outside S.

$$J_{C_{2,1}} = \Big\{ \frac{2315250}{529}, 8000, \frac{148877000}{4761}, \frac{135559106353}{5037138}, 287496, \frac{135638288072}{42849}, \frac{545138290809}{16928}, \frac{3065617154}{9}, \frac{870436774592}{204004089}, \frac{953312}{529}, 1728, \frac{39304000}{14283}, \frac{115387499277504}{148035889}, \frac{13144256}{4761}, 10976, \frac{2744000}{9}, \frac{45989074372}{7555707}, \frac{16000}{3}, \frac{3121792}{1587}, \frac{413493625}{1587}, \frac{140608}{3}, \frac{19307236}{1587}, \frac{50591419971625}{28422890688}, \frac{19056256}{27}, \frac{16879645312}{128547}, \frac{28756228}{3}, \frac{10963069081334500}{1156923}, \frac{21081759765625}{57132}, \frac{949104}{529}, 3456, 54000, \frac{1546167879660104}{323754489243}, \frac{1522096994}{839523}, \frac{3112136}{1587}, \frac{85184}{3}, \frac{143877824}{14283}, \frac{80919167474}{14283}, \frac{7301384}{3}, \frac{3463512697}{3174}, \frac{58591911104}{243}, \frac{1259712}{529}, 23328, \frac{8000}{1863}, \frac{-8000}{9}, \frac{-21296}{729}, \frac{13500}{23}, \frac{-35152}{1863}, \frac{-171879616}{150903}, \frac{1640689628}{12223143}, \frac{-14647977776}{59049}, \frac{2924207}{3312}, \frac{-116930169}{23552}, \frac{-28756228}{16767}, \frac{21296}{207}, \frac{314432}{207}, \frac{17576000}{16767}, \frac{-2924207}{81}, \frac{-10627137250000}{110008287}, \frac{4}{9}, \frac{-389017}{828}, \frac{-15625}{207}, \frac{30289632400448}{58194383823}, \frac{-4956477625}{268272}, \frac{752329532375}{448524288}, \frac{107850176}{16767}, \frac{3370318}{81}, \frac{1666957239793}{301806}, \frac{209254496}{207}, \frac{65939264}{1863}, \frac{7377976076947776}{12167}, \frac{2491343456}{1358127}, \frac{13289344}{23}, \frac{12214672127}{9}, \frac{4499456}{27}, \frac{2048}{3}, \frac{61604313088}{621}, \frac{15043017316604}{243}, \frac{3538944}{23}, \frac{6859000}{3}, \frac{1378334691074}{69}, \frac{51478848}{23}, 0, \frac{545338513}{171396}, \frac{1556068}{81}, \frac{170769126592}{281132289}, 128, \frac{-8000}{81}, \frac{4135597648}{385641}, \frac{4000}{9}, \frac{21952}{9}, \frac{-219488}{729}, \frac{35152}{9}, \frac{676449508}{4761}, \frac{64}{9}, \frac{-873722816}{59049}, \frac{207646}{6561}, \frac{97336}{81} \Big\}$$

At the end we have 97 isomorphism classes[5] with 1664 elliptic curves. The

[5]We include curves for $j = 0, 1728$. For $j = 0$ there are curves with good reduction outside $\{2, 3, 23\}$ 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

$$G_\lambda = \left[-1, \phi^2 - \phi - 1, \phi + 1\right] \qquad G_\mu = \left[-1, -\phi, \phi^2 - 2\right]$$

All the generators of G_λ and G_μ are in $\mathcal{O}_K^*$. By the reduction step we have that[6] 35 is an upper bound of the absolute value of the exponents of the free part of G_λ and G_μ. So, $B_0 = (2, 35, 35)$. Since S_λ and S_μ 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 λ. Then a simple loop computes W_λ which is

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

From this set of W_λ 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 $2742336 = 2^6 3^4 23^2$.

[6] In practice it seems that we get 'small' upper bounds from the reduction step when all the generators of G_λ and G_μ 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 $\mathrm{rank}(G_\lambda) = \mathrm{rank}(G_\mu)$ 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

$$
\begin{aligned}
G_\lambda = \Big[& -1, -\frac{4}{69}\psi\xi^2 + (\frac{1}{23}\psi + 1)\xi + \frac{3}{46}\psi + \frac{1}{2}, (-\frac{3}{23}\psi + 3)\xi^2 + (\frac{8}{23}\psi - 6)\xi \\
& + \frac{1}{46}\psi - \frac{11}{2}, (-\frac{1}{276}\psi + \frac{1}{4})\xi^2 + \frac{3}{46}\psi\xi + \frac{9}{92}\psi - \frac{5}{4}, (\frac{15}{23}\psi - \frac{63}{23})\xi^2 \\
& + (-\frac{28}{23}\psi + \frac{168}{23})\xi - \frac{32}{23}\psi - \frac{1}{23} \Big] \\
G_\mu = \Big[& -1, \frac{4}{69}\psi\xi^2 + (-\frac{1}{23}\psi - 1)\xi - \frac{3}{46}\psi + \frac{1}{2}, (-\frac{9}{23}\psi - 3)\xi^2 + (\frac{1}{23}\psi + 3)\xi \\
& + \frac{95}{46}\psi + \frac{37}{2}, (\frac{1}{69}\psi - \frac{1}{2})\xi^2 + (-\frac{1}{92}\psi + \frac{1}{4})\xi - \frac{13}{92}\psi + \frac{7}{4}, (\frac{18}{23}\psi + \frac{132}{23})\xi^2 \\
& + (-\frac{14}{23}\psi - \frac{30}{23})\xi - \frac{100}{23}\psi - \frac{781}{23} \Big]
\end{aligned}
$$

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_λ and G_μ. So, $B_0 = (2, 663, 663, 663, 663)$. There are 3 primes above 2 and 23 and one prime above 3 in L. Thus $g_{\mathfrak{B}} = 3$ for all $\mathfrak{B} \in S_\lambda, S_\mu$. By proving the non–existence of solutions of the inequality $|\mu - 1|_{\mathfrak{B}} < \delta$ for suitable choice of $\mathfrak{B} \in S_\lambda \setminus S_\mu$ and δ we have that $B_1 = (2, 663, 663, 64, 31)$.

We continue by applying the results of Section 6.2 and we end up with $B_2 = (2, 247, 226, 64, 31)$. Now we are not able to prove that all the sets $\mathcal{T}^6_{\mathfrak{B}}$ 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 $\mu \equiv 1 \mod (\mathfrak{B}_2)^4$ 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 6.2 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

$$\{244465700076/23, 78732/23, 11943936/23, 46656/23, 105456/23, 11664,$$
$$49152/23, 6144, 5719872/23, 55296/23, 1492992/23, 6962820672/23,$$
$$90853097472/23\}$$

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_λ

and G_μ 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.

$$J_{S_3} = \Big\{ \frac{-605310849}{1024}, 207, -26496, \frac{-313994137}{64}, \frac{-1550640289}{1327104}, \frac{92}{81}, \frac{11265584}{6561},$$
$$\frac{-149122432}{59049}, \frac{-152827456}{81}, \frac{23}{4}, -2116, -9936, \frac{-2944}{9}, 1472, \frac{-412313472}{529},$$
$$\frac{-33060921612804657}{8875147264}, \frac{490609013103}{37897187584}, \frac{-15944049}{8464}, \frac{766656}{529}, \frac{109503}{64}, -36,$$
$$-316368, \frac{-35937}{4}, 1152, -784446336, 432, -576, -3456, -4408272, 828,$$
$$\frac{-42592000}{12167}, \frac{-1149984000}{23}, \frac{-562432}{23}, \frac{-6912}{23}, \frac{-256}{23}, \frac{32000}{23}, 256, -268272,$$
$$276, \frac{261685248}{279841}, \frac{-746496}{529}, -12288000, -3072, 1536, -13824, \frac{-11776000}{2187},$$
$$\frac{-188416}{3}, \frac{23552}{27}, \frac{-1190106112}{243}, \frac{-76877424}{279841}, \frac{-165888}{529}, \frac{-3207469280919552}{279841},$$
$$\frac{820125}{529}, \frac{-3472875}{4}, \frac{10125}{64}, -5184, -497664, -972, 1296, \frac{-57032019}{256}, \frac{5589}{4},$$
$$\frac{-1990656}{529}, -41472, \frac{-3556224000}{279841}, -82944, \frac{21233664}{12167}, \frac{5831294976}{23}, \frac{248832}{23},$$
$$\frac{41472}{23}, \frac{4269861568512}{23}, 41472, \frac{60466176}{23}, \frac{149721291}{48668}, \frac{620663201409024}{3404825447},$$
$$\frac{121697237568}{12167}, \frac{23892339312}{6436343}, \frac{618470208}{12167}, \frac{107986944}{12167}, \frac{651245403}{376832}, \frac{1601613}{64},$$
$$\frac{1167051}{23}, \frac{1860867}{368}, \frac{6848175699}{1472}, 311469, \frac{244465700076}{23}, \frac{78732}{23}, \frac{11943936}{23},$$
$$\frac{46656}{23}, \frac{105456}{23}, 11664, \frac{49152}{23}, 6144, \frac{5719872}{23}, \frac{55296}{23}, \frac{1492992}{23}, \frac{6962820672}{23},$$
$$\frac{90853097472}{23}, \frac{881443109376}{12167}, \frac{82944}{23}, 995328, \frac{1119744}{23}, \frac{30233088}{12167}, \frac{331776}{23},$$
$$6718464, \frac{124416}{23}, \frac{663552}{23}, \frac{9553933007697822 72}{23}, \frac{-2817559698624}{12167}, 3,$$
$$\frac{-55699202259}{25745372}, \frac{-6545475219}{23552}, \frac{37044}{23}, \frac{-3456}{23}, \frac{-105456}{23}, \frac{-77625}{512}, -9522,$$
$$\frac{-2057243625}{8}, -39744, 1656, \frac{989120151}{1083392}, \frac{-140625}{8}, \frac{-189613868625}{128}, 576,$$

$$\frac{-1159088625}{2097152}, \frac{42876576}{279841}, \frac{27000}{529}, \frac{-8947094976}{529}, -864, -72000, -72, \frac{3375}{2},$$
$$-39091613782464, \frac{-97967097}{128}, 46, -17950304, -1472, -32800284428081472,$$
$$-621000, \frac{207}{2}, \frac{-64701513}{97336}, \frac{6128487}{11776}, \frac{-1728}{23}, \frac{-18}{23}, 72, -69931566, \frac{-8579808}{23},$$
$$\frac{1193859}{512}, \frac{94531131}{8}, \frac{107811}{8}, 4374, 1944, 5184, 15552, 2592, \frac{555579}{2}, 419904,$$
$$15786448344, \frac{-504896}{243}, \frac{-29393898574784}{177147}, \frac{-20285403817}{279936}, \frac{621}{32}, \frac{33856}{27}, \frac{184}{3},$$
$$\frac{-778918741604594}{27}, -19872, \frac{-1602604156632}{529}, \frac{-11088125088}{279841}, \frac{1811338924224}{78310985281},$$
$$\frac{65856}{529}, \frac{-3721734}{529}, \frac{1249243533}{1083392}, \frac{9261}{8}, \frac{-1167051}{512}, -1728, -216, -6, \frac{-132651}{2},$$
$$-21024576, -32928, 192, 864, \frac{-150160511907}{536870912}, 552, -426006, \frac{8117781}{32768}, \frac{-1587}{2},$$
$$\frac{-18500211}{32}, 1242, -4416, \frac{-911925409752}{6436343}, \frac{750141}{736}, \frac{-2592}{23}, -972000, \frac{-1728}{12167},$$
$$\frac{-91125}{8}, \frac{-2890629687594173619}{12947848928690176}, \frac{-2334102}{23}, \frac{9261}{46}, \frac{-46656}{23}, \frac{12000}{23}, \frac{-4522138875}{389344},$$
$$\frac{1302328125}{753664}, 486, \frac{-15552}{23}, \frac{-2187}{46}, \frac{-57176858301606}{23}, \frac{-182095371}{2944}, \frac{666792}{12167}, \frac{20250}{23},$$
$$\left.\frac{-2791300500000}{23}, \frac{-209952}{23}, 0, -3815424\right\}$$

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[8] isomorphism classes with 3808 curves and maximal conductor $32908032 = 2^8 3^5 23^2$.

To sum up, for $K = \mathbb{Q}$ and $S = \{2, 3, 23\}$ we have found[9] 312 isomorphism classes and 5520 curves.

[8] Including $j = 0$.

[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 λ or μ 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[10] 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])

[10]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 Rechnitzer 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 $\mathcal{E}_{K,S}$ 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],

[Wil97], [EG16]). 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 λ–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[1] of the author,

`https://sites.google.com/site/angeloskoutsianas/`

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

[1]The homepage may have changed.

Bibliography

[BR16] M. A. Bennett and A. Rechnitzer. Computing elliptic curves over $\mathbb{Q}$: bad reduction at one prime. 2016. Personal communication.

[BSD63] B. J. Birch and H. P. F. Swinnerton-Dyer. Notes on elliptic curves. I. *J. Reine Angew. Math.*, 212:7–25, 1963.

[BSD65] B. J. Birch and H. P. F. Swinnerton-Dyer. Notes on elliptic curves. II. *J. Reine Angew. Math.*, 218:79–108, 1965.

[CL07] J. E. Cremona and M. P. Lingham. Finding all elliptic curves with good reduction outside a given set of primes. *Experiment. Math.*, 16(3):303–312, 2007.

[Coh93] Henri Cohen. *A course in computational algebraic number theory*, volume 138 of *Graduate Texts in Mathematics*. Springer-Verlag, Berlin, 1993.

[Coh00] Henri Cohen. *Advanced topics in computational number theory*, volume 193 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2000.

[CPV16] J. Cremona, A. Pacetti, and N. Vescovo. Computing rational elliptic curves. 2016. preprint.

[Cre97] J. E. Cremona. *Algorithms for modular elliptic curves*. Cambridge University Press, Cambridge, second edition, 1997.

[Dev16] The Sage Developers. *Sage Mathematics Software (Version 7.0)*, 2016. `http://www.sagemath.org`.

[EG16] Jan-Hendrink Evertse and Kálmán Győry. *Unit Equations in Diophantine Number Theory*. Cambridge Studies in Advanced Mathematics. Cambridge University Press, 2016.

[Eve84] J. H. Evertse. On equation in S-units and the Thue–Mahler equation. *Inventiones mathematicae*, 75:561–584, 1984.

[FP85] U. Fincke and M. Pohst. Improved methods for calculating vectors of short length in a lattice, including a complexity analysis. *Math. Comp.*, 44(170):463–471, 1985.

[JR14] John W. Jones and David P. Roberts. A database of number fields. *LMS J. Comput. Math.*, 17(1):595–618, 2014.

[LLL82] A. K. Lenstra, H. W. Lenstra, Jr., and L. Lovász. Factoring polynomials with rational coefficients. *Math. Ann.*, 261(4):515–534, 1982.

[LMF16] The LMFDB Collaboration. The L–functions and Modular Forms Database. `http://www.lmfdb.org`, 2016. [Online; accessed 1 August 2016].

[Neu99] Jürgen Neukirch. *Algebraic number theory*, volume 322 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, 1999. Translated from the 1992 German original and with a note by Norbert Schappacher, With a foreword by G. Harder.

[NSW08] Jürgen Neukirch, Alexander Schmidt, and Kay Wingberg. *Cohomology of number fields*, volume 323 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, second edition, 2008.

[PAR16] The PARI Group, Bordeaux. *PARI/GP version* `2.7.0`, 2016. available from `http://pari.math.u-bordeaux.fr/`.

[PZGH99] Attila Pethő, Horst G. Zimmer, Josef Gebel, and Emanuel Herrmann. Computing all S-integral points on elliptic curves. *Math. Proc. Cambridge Philos. Soc.*, 127(3):383–402, 1999.

[Rib76] Kenneth A. Ribet. A modular construction of unramified p-extensions of $Q(\mu_p)$. *Invent. Math.*, 34(3):151–162, 1976.

[Sil86] Joseph H. Silverman. *The Arithmetic of Elliptic Curves*, volume 106 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1986.

[Sil94] Joseph H. Silverman. *Advanced topics in the arithmetic of elliptic curves*, volume 151 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1994.

[Sma95] N. P. Smart. The solution of triangularly connected decomposable form equations. *Math. Comp.*, 64(210):819–840, 1995.

[Sma98] Nigel P. Smart. *The algorithmic resolution of Diophantine equations*, volume 41 of *London Mathematical Society Student Texts*. Cambridge University Press, Cambridge, 1998.

[Sma99] N. P. Smart. Determining the small solutions to S-unit equations. *Math. Comp.*, 68(228):1687–1699, 1999.

[ST94] R. J. Stroeker and N. Tzanakis. Solving elliptic Diophantine equations by estimating linear forms in elliptic logarithms. *Acta Arith.*, 67(2):177–196, 1994.

[Ste91] William A. Stein. *The Birch and Swinnerton–Dyer Conjecture, a Computational Approach*. 1991.

[TdW89] N. Tzanakis and B. M. M. de Weger. On the practical solution of the Thue equation. *J. Number Theory*, 31(2):99–132, 1989.

[TW92] N. Tzanakis and B. M. M. de Weger. How to explicitly solve a Thue–Mahler equation. *Compositio Mathematica*, 84(3):223–288, 1992.

[Weg87] B. M. M. de Weger. Solving exponential Diophantine equations using lattice basis reduction algorithms. *J. Number Theory*, 26(3):325–367, 1987.

[Weg88] B. M. M. de Weger. *Algorithms For Diophantine Equations*. PhD thesis, University of Leiden, 1988.

[Wil97] K. Wildanger. *Über das Lösen von Einheiten– und Indexformgleichungen in algebraischen Zahlkörpern mit einer Anwendung auf die Bestimmung aller ganzen Punkte einer Mordellschen Kurve.* PhD thesis, Technischen Universität Berlin, 1997.

[Wil00] K. Wildanger. Über das Lösen von Einheiten- und Indexformgleichungen in algebraischen Zahlkörpern. *J. Number Theory*, 82(2):188–224, 2000.