THE UNIVERSITY OF
WARWICK

AUTHOR: **Carlos Filipe Barros** DEGREE: **Ph.D.**

TITLE: **On the Lebesgue-Nagell equation and related subjects**

DATE OF DEPOSIT: .....

I agree that this thesis shall be available in accordance with the regulations governing the University of Warwick theses.

I agree that the summary of this thesis may be submitted for publication.

I **agree** that the thesis may be photocopied (single copies for study purposes only).

Theses with no restriction on photocopying will also be made available to the British Library for microfilming. The British Library may supply copies to individuals or libraries. subject to a statement from them that the copy is supplied for non-publishing purposes. All copies supplied by the British Library will carry the following statement:

> "Attention is drawn to the fact that the copyright of this thesis rests with its author. This copy of the thesis has been supplied on the condition that anyone who consults it is understood to recognise that its copyright rests with its author and that no quotation from the thesis and no information derived from it may be published without the author's written consent."

AUTHOR'S SIGNATURE: .....

USER'S DECLARATION

1. I undertake not to quote or make use of any information from this thesis without making acknowledgement to the author.
2. I further undertake to allow no-one else to use this thesis while it is in my care.

DATE SIGNATURE ADDRESS

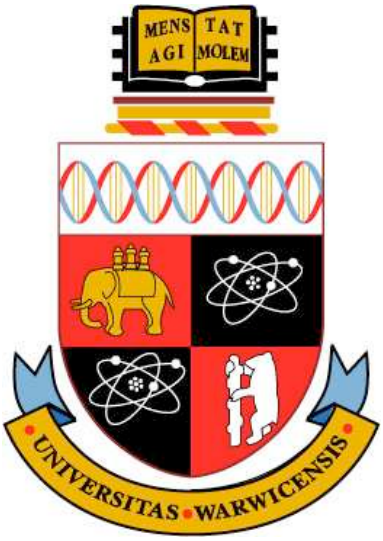
.....

.....

.....

.....

.....



On the Lebesgue-Nagell equation and related subjects

by

Carlos Filipe Barros

Thesis

Submitted to the University of Warwick

for the degree of

Doctor of Philosophy

Mathematics

August 2010

THE UNIVERSITY OF
WARWICK

Florinda,

Se sou o que sou, se cheguei aonde cheguei, a ti o devo. Estarás sempre no meu coração e no meu pensamento, estejas onde estiveres! Um beijo enorme do teu

Filipe

Contents

List of Tables

Acknowledgments

First of all, I would like to thank Samir Siksek, for being my supervisor for the past four years and for his invaluable support and constructive criticism for the writing of this thesis. I have learned a lot from his deep knowledge of Number Theory.

I would also like to thank the Number Theory group at Warwick Mathematics Institute for their valuable advice and helpful discussions.

Many thanks to my good friends, who kept me going. In particular Ana Maria, Ana Cristina, Maite, Dany, Rui, Nook, Anna Morra, Nuno, my Warwick Family, Marta, Jorge, José, Susana, Francisco, Daniel, Ruben, Cristina. Never forgetting the friends from the very beginning to the most recent ones. Thank you for being part of this journey.

To my parents, who have supported me through all this hard labour; my grandmother, godparents, uncle, cousins and the rest of my family, who have always encouraged all through out this time.

Finally, I thank FCT- Fundação para a Ciência e Tecnologia - for their financial support through the PhD grant with reference SFRH/BD/ 29433 / 2006

Declarations

I declare that, to the best of my knowledge and unless otherwise stated, all the work in this thesis is original. I confirm that this thesis has not been submitted for a degree at another university.

Abstract

The work of Cohn [Coh93] and Bugeaud, Mignotte and Siksek [BMS06] solves the Lebesgue-Naguel equation

$$x^2 + D = y^n, \quad x, y \text{ integers }, n \geq 3$$

for D a integer in the range $1 \leq D \leq 100$. We propose to do the same for D in the range $-100 \leq D \leq -1$. For that we will use techniques that go from the most classical ones, ideal factorization over number fields and Thue equations, to the most modern approach to Diophantine equations, Frey curves and the Modular approach, passing by linear forms in logarithms.

Chapter 1

Introduction

The main purpose of this thesis is explicitly solving Diophantine equations, in particular the Lebesgue–Nagell equations,

$$x^2 + D = y^n, \tag{LN}$$

where D is a non-zero integer, x, y integer unknowns and n also an integer unknown, greater than or equal to 2. We will be especially interested in solving these equations via the modular method, but we will also use other methods, whenever the modular method seems to fail, or when there are better methods to determine all the solutions for our equations, usually given a value for n.

1.1 A brief account of the history of the Lebesgue-Nagell equations

The history of the Lebesgue-Nagell equation (**LN**) is very rich: there are literally hundreds of papers devoted to special cases of this equation. Most of this literature is concerned with the case $D > 0$, and either for special values of n or of y, usually given a specific value for D. For example, for $D = 2$ and $n = 3$, Fermat asserted

that he had shown that the only solutions are given by $x = 5, y = 3$; a proof was given by Euler [Eul70].

The equation (**LN**) with $n = 3$ is the intensively studied Mordell equation (see [Mor69] or [GPZ98] for a modern approach). There are also some results known for the special cases $n = 5$ (see [Bla76], [Wre73], [Sto06]) and $n = 7$ (see [BS78]). For a general D and general n, the work of Cohn [Coh93] and of Bugeaud, Mignote, Siksek [BMS06] provides us solutions for D in the range $1 \leq D \leq 1000$. Stoll has also studied this equation but on an arithmetic point of view, see [Sto98] and [Sto02].

Another notable particular case is the generalized Ramanujan-Nagell equation:

$$x^2 + D = k^n, \qquad \textbf{(GRN)}$$

where D and k are given integers. This is an extension of the Ramanujan-Nagell equation $x^2 + 7 = 2^n$, proposed by Ramanujan in 1913, [Ram13], and first solved by Nagell in 1948, [Nag48] (see also the collected papers of Nagell [Nag02]). This equation has exactly five solutions with $x \geq 1$ (see [Mig84] for a very simple proof) and is in this respect singular: indeed, Bugeaud and Shorey established that equation (**GRN**) with positive D and k a prime number not dividing D has at most two solutions in positive integers x, n, except for $(D, k) = (7, 2)$. They also listed all the pairs (D, k) as above for which equation (**GRN**) has exactly two solutions. Much earlier, Apéry,(see [Apé60a] and [Apé60b]), proved by p-adic arguments that the equation (**GRN**), with k prime, has at most two positive integer solutions except if $(D, k) = (7, 2)$.

The first result for general y, n, regarding the equation (**LN**), seems to be the proof in 1850, by Lebesgue [Leb50] that there are no non-trivial solutions for $D = 1$; by non-trivial we mean $xy \neq 0$, for we always have the solution

$(x, y) = (0, 1)$ when n is odd and $(x, y) = (0, \pm 1)$ when n is even. The next cases to be solved were $D = 3, 5$ by Nagell [Nag48] in 1923. It is for this reason that equation (**LN**) is called Lebesgue-Nagell equation in [BMS06]. Nagell also had provided a non-complete proof for the case $D = 2$. This case was finally solved by Ljunggren [Lju43], generalizing the result of Fermat and proving that there is no solution other than $x = 5$. This was also rediscovered by Nagell in 1954 (see [Nag54]). The case with $D = -1$ is particularly noteworthy: a solution was sought for many years as a special case of the Catalan conjecture. This case was finally settled by Chao Ko [Ko64] in 1965.

Cohn [Coh93] solved equation (**LN**) for 77 values of $1 \leq D \leq 100$. For $D = 74, 86$ the equation was solved by Mignotte and de Weger [MdW96] using linear forms in logarithms and Bennett and Skiner [BS04] solved it for $D = 55, 95$. One of the remaining 19 values of $1 \leq D \leq 100$, was $D = 7$, a generalization of the Ramanujan-Nagell equation. In [Coh93] Cohn, proposed that the only solutions to

$$x^2 + 7 = y^n, \tag{RN}$$

where the solutions of the Ramanujan-Nagell equation and some "rearrangements" of these solutions. In the same paper Cohn showed that there could be no solutions with y odd, nor with n even nor with $3 \mid n$. In [Les98] Lesage proves various partial results concerning this equation, in particular if (x, y, n) is a solution of(**RN**) then $n \leq 6.6 \times 10^{15}$, using linear forms in logarithms. In 2003 Siksek and Cremona [CS03], gave a partial solution to this problem, showing through modular methods, that there is no solution to (**RN**) with n a prime number and $11 \leq n \leq 10^8$. In 2006 Bugeaud, Mignotte and Siksek [BMS06] finally solve this equation as well asthe remaining 18 values of $1 \leq D \leq 100$ for the equation (**LN**).

It is possible to generalize this equation a bit more. Let D_1, D_2, D_3 be

integers, with D_1 positive and square-free, D_3 also a positive integer, then by the generalized Lebesgue-Ramanujan-Nagell equation we mean the following equation:

$$D_1x^2 + D_2 = D_3y^n \qquad \textbf{(GLRN)}$$

where x and y are integers and n an integer greater that or equal to 2.

When $D_1 = D_3 = 1, D_2 = D$ and $y = k$ are fixed in (**GLRN**), the resulting equation is the so called Ramanujan-Nagell type equation. While when we fix $D_1 = D_3 = 1, D_2 = D$, we have the Lebesgue-Nagell equation type. For an account on the results known about this generalized equation see [SS08], [BS01], [Sho06].

1.2 Why study this equation?

Reading carefully the history of the Lebesgue-Nagell equation, one thing that strikes the eye is that the majority of the cases so far solved have in common the fact of D being positive. Apart from $D = -1$ and some cases when $D = -d^2$, with d an integer, much less is known. In [Coh93], Cohn states that most of the methods used in that paper can be applied also to the case when D is negative, but refrains himself from doing so mainly due to the existence of fundamental units in real quadratic number fields.

Suppose $-D$ is not a square, if we consider the left-hand side of (**LN**), we can factorize it in the following way

$$x^2 + D = (x + \sqrt{-D})(x - \sqrt{-D}).$$

This factorization is possible over the number field $\mathbb{Q}(\sqrt{-D})$. Therefore when D is negative we obtain a real quadratic number field, which always has a fundamental unit. While on the other hand, when D is positive we obtain an imaginary quadratic

number field, which has always finitely many units. In fact at most we will have 6 units to deal with.

Now to answer the question in the title of this section, I state that the main purpose of this thesis is to overcome this gap in the literature. I will show how to apply the already mentioned methods in the literature, with the appropriate changes and when needed, with new tricks, to try to find all the solutions, *when possible*, for the equation (**LN**) in the range

$$-100 \leq D \leq -1. \tag{R}$$

1.3 Thesis outline and main result

The main result of this thesis is the following

Theorem 1.1. *All solutions to equation* (**LN**) *with* D *in the range* (**R**) *are given in the Tables A.1 and A.2, pages 206-209 , with the following exceptions:*

(1) For the values of D *in Table 1.1, when* n *is divisible by a prime number* p*, such that* $10^8 < p \leq p_{max}$*, where* p_{max} *is given in Table 1.1, we do not know if there are any solutions or not to equation* (**LN**)*. If* n *is divisible by a prime* $p < 10^8$ *or* $p > p_{max}$*, then the solutions are given in the Table A.2.*

(2) For the values of D *in table 1.2, when* n *is divisible by a prime number* p*, such that* $13 < p \leq p_{max}$*, where and* p_{max} *is given in Table 1.1, we do not know if there are more solutions or not to equation* (**LN**)*, apart from the one that ones already given in Table 1.2 and Table A.2. As before, if* n *is divisible by a prime* $p \leq 13$ *or* $p > p_{max}$*, then the solutions are given in the Table A.2.*

Table 1.1: First exceptional values of D

D	p_{max}
-33	157 752 030 294
-41	359 940 708 129
-57	429 407 772 757
-68	16 382 452 021
-73	808 303 621 445
-90	29 188 841 666
-97	2 552 797 449 913
-98	8 383 577 486

Table 1.2: Second exceptional values of D

D	p_{max}	$(\|x\|, y, n^a)$
-2	4 111	$(1, -1, p)$
-3	7 793	$(2, 1, p)$
-5	1 759	$(2, -1, p)$
-8	4 111	$(3, 1, p)$
-10	13 291	$(3, -1, p)$
-15	16 433	$(4, 1, p)$
-17	40 902 094 178	$(4, -1, p)$
-24	19 687	$(5, 1, p)$
-26	19 979	$(5, -1, p)$
-35	22 483	$(6, 1, p)$
-37	22 709	$(6, -1, p)$
-48	7 703	$(7, 1, p)$
-50	4 111	$(7, -1, p)$
-63	69 516 630 329	$(8, 1, p)$
-65	49 434 815 608	$(8, -1, p)$
-80	1 759	$(9, 1, p)$
-82	29 423	$(9, -1, p)$
-99	31 223	$(10, 1, p)$

[a] where n is divided by primes between 13 and p_{max}

In Chapter 2 we will use mainly methods coming from algebraic number theory, especially the unique factorization of ideals in number fields to solve our equations. We will show how to get from a possible solution of the equation (**LN**) to a Thue equation. The main improvement in these areas comes from using Selmer groups to construct the Thue equations and the development of local and global methods to help us solve these new equations. These methods will be used to solve equation (**LN**) for a given $n \geq 3$. For $n = 2$ or a multiple of 2 we will also expose how to obtain solutions for equation (**LN**) using more simple techniques. We will also use some methods already known from the study of elliptic curves,

especially methods to find all the integral points on a elliptic curve. The methods coming from elliptic curves will be used to find all the solutions for (**LN**) when $n = 3$ or a multiple of 3.

Chapter 3 is dedicated to the modular approach. We will give a brief introduction to the modular approach and see how these new techniques will help us to solve our equations, assuming that n is a prime greater than or equal to 7. For this we will be following the work of Ivorra and Kraus [IK06], on the study of certain Frey curves, and expand some of the work already presented in [BMS06].

When it is not possible to find all the solutions to (**LN**) for a given value of D within our range (**R**) we will need to use other methods. So in Chapter 4 we will just make a brief introduction to linear forms in two and three logarithms. We will follow mainly the results and techniques of Matveev (see [Mat00]) for the general case, and those of Laurent, Mignotte and Nesterenko (see [LMN95]) for the two logarithms case and Mignotte (see [Mig08]) for the three logarithms case. With this method we will try to solve the cases left unsolved by the modular approach.

In Chapter 5 we will introduce a new Frey curve associated to a particular ternary Diophantine equation, and see how it can help solving the equation (**LN**).

The last part of this thesis contains tables with the solutions for the cases already solved and the algorithms that were used to solve our equations.

1.4 Notation

Though most notation is quite standard and will not be mentioned here, we would like to mention the following.

Given $n \in \mathbb{Z} \setminus \{0\}$ we denote by $\mathrm{Rad}(n)$ the product of primes dividing n. For S a finite set of primes of $\mathbb{Z}$, then $\mathrm{Rad}_S(n)$ denotes the products of the primes

dividing n that are not in S. If $S = \{p\}$, for a prime p then instead of writing $\mathrm{Rad}_S(n)$ we write $\mathrm{Rad}_p(n)$. Given a prime p and r a non-zero rational number we will denote by $v_p(r)$ the p-valuation of r.

Let $\mathbb{K}$ be a number field and $\mathfrak{a}$ an ideal of $\mathbb{K}$. By $\mathcal{N}(\mathfrak{a})$ we understand the norm of the ideal $\mathfrak{a}$. By $S(\mathfrak{a})$ we denote the set of all prime ideals $\mathfrak{p}$ that divide $\mathfrak{a}$. If $\mathfrak{b}$ is another ideal we denote by $S(\mathfrak{a} \setminus \mathfrak{b})$ the set $S(\mathfrak{a}) \setminus S(\mathfrak{b})$. If $\alpha, \beta \in \mathbb{K}$ then we denote by $S(\alpha)$ and $S(\alpha \setminus \beta)$ respectively, the sets $S(\langle\alpha\rangle)$ and $S(\langle\alpha\rangle \setminus \langle\beta\rangle)$. We will denote by $\mathfrak{O}_{\mathbb{K}}, U_{\mathbb{K}}, \mu_{\mathbb{K}}, Cl_{\mathbb{K}}$ the ring of integers, the unit group, the torsion subgroup, and the class group of $\mathbb{K}$, respectively. For an elliptic curve E defined over $\mathbb{Q}$, denoted by $E/\mathbb{Q}$, the conductor will be denoted by N_E, the minimal discriminant by $\Delta_{\mathsf{min}}(E)$ and the j-invariant by j_E. If E is given by a specific Weierstrass equation, then the discriminant of this Weierstrass equation is denoted by Δ_E. If no confusion should arise, sometimes we will simply just use $N, \Delta_{\mathsf{min}}, j$ and Δ. Given a prime p, the set of points on the reduction of E modulo p is denoted by $E(\mathbb{F}_p)$ and we define $a_p(E) := p + 1 - \#E(\mathbb{F}_p)$.

Let $\mathbb{K}$ be a field, we fix an algebraic closure $\overline{\mathbb{K}}$ of $\mathbb{K}$ and we assume implicitly that all algebraic extensions and all elements are chosen in this algebraic closure. Since $\mathbb{C}$ is an algebraically closed field, we consider $\overline{\mathbb{Q}}$ to be the algebraic closure of $\mathbb{Q}$ in $\mathbb{C}$.

Finally, $\mathcal{G}_{\mathbb{Q}}$ will denote the absolute Galois group $Gal(\overline{\mathbb{Q}}/\mathbb{Q})$.

Chapter 2

Classical methods to solve Diophantine equations

Though most of the work here can be done for a general integer $n \geq 2$, in some cases we will consider n to be a prime. So for this reason we will be considering instead the equation:

$$x^2 + D = y^p, \tag{2.1}$$

where p is a prime number, and x, y and D are as before. Still we will try to be as general as possible. In fact we still start looking at the most general case, the generalized Lebesgue-Ramanujan-Nagell equation (**GLRN**) and go from there. But when needed, or when the general case becomes too difficult to overcome, we will go back to our starting point (**LN**) or (2.1).

2.1 A few facts concerning algebraic number theory

Most of the facts, definitions and results we might use from algebraic number theory are well known and can be found in [Coh07a], [IR82] and [ST87].

We will just provide a brief exposition concerning Hensel's lemma.

2.1.1 Hensel's lemmas

Let $\mathbb{K}$ be a number field, $\mathfrak{O}_{\mathbb{K}}$ its ring of integers. Let $\mathfrak{p}$ be a finite place of $\mathbb{K}$ and $\mathbb{K}_{\mathfrak{p}}$ the associated $\mathfrak{p}$-adic field, with ring of integers $\mathbb{Z}_{\mathfrak{p}}$. It is possible to develop a theory of analytic functions in $\mathfrak{p}$-adic fields, but we will be more interested in one of the most crucial tools that allows us to work in $\mathfrak{p}$-adic fields, called *Hensel's lemma*, which is a simple result, in fact is nothing else than a non-Archimedean version of Newton's root-finding method. We begin with the following result, where for any object x, we denote by $\overline{x}$ the reduction of x modulo $\mathfrak{p}$. We will identify $\mathbb{Z}_{\mathfrak{p}}/\mathfrak{p}\mathbb{Z}_{\mathfrak{p}}$ with $\mathfrak{O}_{\mathbb{K}}/\mathfrak{p}$.

Proposition 2.1.1 (Hensel's lemma version I). *Let $f \in \mathbb{Z}_{\mathfrak{p}}[X]$, and assume that $\overline{f}(x) = \phi_1(X)\phi_2(X)$ with $\phi_i \in (\mathfrak{O}_{\mathbb{K}}/\mathfrak{p})[X]$ coprime. There exist polynomials $f_1, f_2 \in \mathbb{Z}_{\mathfrak{p}}[X]$ such that $f(X) = f_1(X)f_2(X)$, $\overline{f}_i(X) = \phi_i(X)$, and $\deg(f_1) = \deg(\phi_1)$.*

Another version of Hensel's lemma which is very useful to show the existence of roots in $\mathfrak{p}$-adic fields, is the following one.

Proposition 2.1.2 (Hensel's lemma version II). *Let $f \in \mathbb{Z}_{\mathfrak{p}}[X]$ be a monic polynomial and let $\alpha \in \mathbb{Z}_{\mathfrak{p}}$ be such that $|f(\alpha)|_{\mathfrak{p}} < |f'(\alpha)|_{\mathfrak{p}}^2$, where $f'(X)$ is the formal derivative of $f(X)$. There exists a unique root $\tilde{\alpha}$ of $f(X) = 0$ in $\mathbb{Z}_{\mathfrak{p}}$ such that*

$$|\tilde{\alpha} - \alpha|_{\mathfrak{p}} \leq \frac{|f(\alpha)|_{\mathfrak{p}}}{|f'(\alpha)|_{\mathfrak{p}}} < |f'(\alpha)|_{\mathfrak{p}}.$$

When $f(\alpha) \in \mathfrak{p}\mathbb{Z}_{\mathfrak{p}}$ and $f'(\alpha)$ is a $\mathfrak{p}$-adic unit, that is, $|f'(\alpha)|_{\mathfrak{p}} = 1$, the condition of the proposition is satisfied. Below is an important consequence. First some definitions.

Definition 2.1.1. *Let $P(X_1, \ldots, X_n) = 0$ be a homogenous polynomial equation. We say that a nontrivial solution $(x_1, \ldots, x_n)$ of the homogenous equation is* nonsingular *if $\frac{\partial P}{\partial X_j}(x_1, \ldots, x_n) \neq 0$ for at least one index j. We say that the equation itself is nonsingular if it has no nontrivial singular solutions.*

Proposition 2.1.3 (Hensel's lemma version III). *Let $P(\underline{X}) \in \mathbb{Z}_{\mathfrak{p}}[X_1, \ldots, X_n]$ be a homogenous polynomial in n variables, and let $(x_1, \ldots, x_n) \in (\mathfrak{O}_{\mathbb{K}}/\mathfrak{p})^n$ be a nontrivial nonsingular solution of $\overline{P}(\underline{X}) = 0$, then there exists $(\alpha_1, \ldots, \alpha_n) \in \mathbb{Z}_{\mathfrak{p}}^n$ satisfying $P(\alpha_1, \ldots, \alpha_n) = 0$ such that $\overline{\alpha}_i = x_i$ for all $i \in \{1, \ldots n\}$.*

For a proof of the three lemmas we refer the reader to section 4.1.7 in [Coh07a].

2.2 Thue equations

We now go back to our equation (**LN**). We will use algebraic methods to find all solutions for a given D in the range (**R**) and $n \geq 2$.

We will now explain how to reduce the equation (**LN**) to Thue equations.

We consider the general case (**GLRN**),

$$D_1 x^2 + D_2 = D_3 y^n,$$

where D_1, D_2, D_3 are nonzero integers. Suppose that (x, y) is a solution of (**GLRN**) for a given $n \geq 2$, then $(D_1 x, y)$ is a solution of the following equation,

$$x^2 + D_1 D_2 = D_1 D_3 y^n,$$

so instead of (**GLRN**) we will be considering the equation

$$x^2 + D = C y^n. \tag{2.2}$$

As before we might have to consider n to be a prime number, so when this is the case we will be considering the following equation:

$$x^2 + D = Cy^p, \tag{2.3}$$

with p a prime number.

So let D and C be nonzero integers. Then there are d, q, nonzero integers, with d a square free integer, $q \geq 1$, such that $D = dq^2$. With this in mind, we have that

$$x^2 + D = (x + q\sqrt{-d})(x - q\sqrt{-d}). \tag{2.4}$$

Let $\mathbb{K}_D = \mathbb{Q}(\sqrt{-d})$ and $\mathfrak{O}_D$ denote its ring of integers. The main result of this section is the following:

Theorem 2.1. *Let D_1, D_2, D_3 and n be as above, let $D = D_1D_2$ and $C = D_1D_3$ and let (x, y) be an integral solution of (2.2). Let $\mathbb{K}_D$, d and q be also as above and let $\{1, \omega\}$ be an integral basis of $\mathfrak{O}_D$, with $\overline{\omega}$ the conjugate of ω over $\mathbb{K}_D$. If $y \neq 0$ then there exists a finite set Γ of pairs $\{\gamma_+, \gamma_-\}$, with $\gamma_\pm \in \mathbb{K}_D$ such that:*

$$x = \frac{1}{2}(\gamma_+(A + B\omega)^n + \gamma_-(A + B\overline{\omega})^n), \tag{2.5}$$

where (A, B) is a solution of the Thue equation

$$2q = \frac{1}{\sqrt{-d}}(\gamma_+(A + B\omega)^n - \gamma_-(A + B\overline{\omega})^n). \tag{2.6}$$

Let us now prove this theorem.

We begin by noticing that though not every $\mathfrak{O}_D$ is a UFD, they all have unique factorization for ideals. So instead of considering the equation (2.2) in terms of integers, let us consider in term of ideals:

$$\langle x^2 + D\rangle = \langle Cy^n\rangle. \tag{2.7}$$

Both ideals are principal ideals and according to what we have seen in (2.4), we can factorize in the following way

$$\langle x + q\sqrt{-d})\rangle\langle x - q\sqrt{-d}\rangle = \langle Cy^n\rangle. \tag{2.8}$$

Denote by $\mathfrak{d}_\pm = \langle x \pm q\sqrt{-d}\rangle$. Using the unique factorization for ideals, we have that

$$\mathfrak{d}_\pm = \mathfrak{a}_\pm \mathfrak{b}_\pm^n, \tag{2.9}$$

where $\mathfrak{a}_\pm, \mathfrak{b}_\pm$ are ideals of $\mathfrak{O}_D$ and $\mathfrak{a}_\pm$ is nth power free.

Let us see which properties they satisfy. First, set σ_d to be the automorphim of the field $\mathbb{K}_D$, such that

$$\sigma_d(\sqrt{-d}) = -\sqrt{-d}.$$

Clearly $\sigma_d \in \mathcal{G}(\mathbb{K}_D/\mathbb{Q})$ and $\sigma_d(\mathfrak{a}_\pm) = \mathfrak{a}_\mp, \sigma_d(\mathfrak{b}_\pm) = \mathfrak{b}_\mp$ since $\sigma_d(\mathfrak{d}_\pm) = \mathfrak{d}_\mp$.

For $\mathfrak{a}$ an ideal of $\mathfrak{O}_D$, let $\overline{\mathfrak{a}} = \sigma_d(\mathfrak{a})$; we say that $\mathfrak{a}$ and $\overline{\mathfrak{a}}$ are conjugate.

Suppose now that $\mathfrak{p}$ is a prime ideal of our ring of integers $\mathfrak{O}_D$ such that $\mathfrak{p}$ divides both ideals $\mathfrak{d}_\pm$, so

(i) we first see that $\mathfrak{p} \mid \langle 2q\sqrt{-d}\rangle$ and $\mathfrak{p} \mid \langle 2x\rangle$.

(ii) secondly we see that $\gcd(\mathfrak{d}_+, \mathfrak{d}_-) \mid \langle 2q\sqrt{-d}\rangle$.

Therefore given a prime ideal $\mathfrak{p}$ of $\mathfrak{O}_D$ dividing $\mathfrak{d}_+$ we have that or

(iii) $\mathfrak{p} \mid \langle 2q\sqrt{-d}\rangle$, or

(iv) $\mathfrak{p} \mid \langle C\rangle$, or

(v) $v_\mathfrak{p}(\mathfrak{d}_+) \equiv 0 \pmod{n}$.

So $\mathfrak{a}_+$ must be of the following form:

$$\mathfrak{a}_+ = \prod_{\mathfrak{p} \in S(2DC)} \mathfrak{p}^{\kappa_\mathfrak{p}},$$

where $0 \leq \kappa_\mathfrak{p} < n$

Taking into account the observations made in the items (i) - (v) we are just looking for $(\kappa_\mathfrak{p})_{\mathfrak{p} \in S(2DC)}$ such that:

(1) $0 \leq \kappa_\mathfrak{p} \leq v_\mathfrak{p}(2qC\sqrt{-d})$, for all $\mathfrak{p} \in S(2DC)$;

(2) $\min\{\kappa_\mathfrak{p}, \kappa_{\overline{\mathfrak{p}}}\} \leq v_\mathfrak{p}(2q\sqrt{-d})$;

(3) $\kappa_\mathfrak{p} + \kappa_{\overline{\mathfrak{p}}} \equiv v_\mathfrak{p}(c) \pmod{n}$.

Item (3) means that $\mathcal{N}(\mathfrak{a}_+) \equiv C$ modul0 nth powers, that is $\mathcal{N}(\mathfrak{a}_+)/C \in (\mathbb{Q}^*)^n$.

With this choice of $\mathfrak{a}_\pm$, we have that our $\mathfrak{b}_\pm$ are such that $\gcd(\mathfrak{b}_+, \mathfrak{b}_-) = \mathfrak{O}_D$. Denote by $\mathcal{L}$ the set of pair of ideals $(\mathfrak{a}, \overline{\mathfrak{a}})$ that satisfy the five conditions above.

Let h be the order of the class group of $\mathfrak{O}_D$ and $\mathfrak{g}_1, \mathfrak{g}_2, \ldots, \mathfrak{g}_h$ be integral ideals, forming a complete set of representatives for its ideal class group. Thus, we know that $\mathfrak{g}_i\mathfrak{b}_+$ is a principal ideal for some $i \in \{1, 2, \ldots, h\}$, therefore $(\mathfrak{g}_i\mathfrak{b}_+)^n$ is also a principal ideal. Since $\mathfrak{d}_+$ is a principal ideal and

$$\begin{aligned}\mathfrak{d}_+ &= \mathfrak{a}_+\mathfrak{b}_+^n \\ &= \mathfrak{a}_+(\mathfrak{g}_i\mathfrak{g}_i^{-1})^n\mathfrak{b}_+^n \\ &= \mathfrak{a}_+\mathfrak{g}_i^{-n}(\mathfrak{g}_i\mathfrak{b}_+)^n\end{aligned}$$

we necessarily must have that $\mathfrak{a}_+\mathfrak{g}_i^{-n}$ is a principal ideal. Notice that $\mathfrak{a}_+\mathfrak{g}_i^{-n}$ is a fractional ideal, not necessarily an integral ideal. Let γ be one of its generators,

and let $A, B \in \mathbb{Z}$ such that $\beta = A + B\omega$ is a generator of $\mathfrak{g}_i\mathfrak{b}_+$, with $\{1, \omega\}$ an integral basis of $\mathfrak{O}_D$. So we must have

$$x + q\sqrt{-d} = \gamma u \beta^n, \tag{2.10}$$

where u comes from a set of representatives of the units modulo nth powers, $U_{\mathbb{K}_D}/U^n_{\mathbb{K}_D}$. Let $\gamma_u = \gamma u$. By item (1), we have that

$$x - q\sqrt{-d} = \overline{\gamma}_u(\overline{\beta})^n. \tag{2.11}$$

So adding and subtracting the two equalities (2.10) and (2.11) we have the following "new" equations:

$$2x = \gamma_u\beta^n + \overline{\gamma}_u(\overline{\beta})^n, \tag{2.12}$$

$$2q\sqrt{-d} = \gamma_u\beta^n - \overline{\gamma}_u(\overline{\beta})^n. \tag{2.13}$$

Now, we can rewrite $\gamma_u\beta^n$ and $\overline{\gamma}_u(\overline{\beta})^n$ in the following form

$$\gamma_u\beta^n = P_1(A, B) + P_2(A, B)\omega,$$
$$\overline{\gamma}_u(\overline{\beta})^n = P_3(A, B) + P_4(A, B)\omega,$$

where $P_1, \ldots, P_4$, are homogenous polynomials of degree n in 2 variables over $\mathbb{Q}$. Due to the fact that $\gamma_u\beta^n$ and $\overline{\gamma}_u(\overline{\beta})^n$ are conjugate to each other we have that $P_i = (-1)^{i+1}P_{i+2}$ for $i = 1, 2$.

Therefore we can rewrite the right-hand side of the equations (2.12) and (2.13) as:

$$\gamma_u\beta^n + \overline{\gamma}_u(\overline{\beta})^n = Q_1(A, B), \tag{2.14}$$

$$\gamma_u\beta^n - \overline{\gamma}_u(\overline{\beta})^n = Q_2(A, B)\sqrt{-d}, \tag{2.15}$$

where Q_i are polynomials in two variables over $\mathbb{Q}$.

So using the information from the equations (2.12), (2.13), the equalities (2.14), (2.15) and the fact that $\{1, \omega\}$ is an integral basis of $\mathbb{K}_D$, we have the following equations:

$$Q_1(A, B) = 2x,$$
$$Q_2(A, B) = 2q$$

The question that arises now is how do we obtain γ_u and β? We have that $\mathfrak{b}_\pm$ is unknown to us, at least from the factorization that we did above, on the other hand, from what we have seen, we can calculate the possibilities for $\mathfrak{a}_\pm$ quite easily. Given an integral ideal $\mathfrak{g}$ of the list of representatives of the class group, we can easily check when $\mathfrak{a}_\pm \mathfrak{g}^{-n}$ is principal or not. As consequence we can compute γ_u and $\overline{\gamma}_u$.

Define Γ' be a set containing a pair of generators $\{\gamma, \overline{\gamma}\}$ for every pair of principal ideals of the form $\mathfrak{a}\mathfrak{g}_i^{-n}$ and $\overline{\mathfrak{a}}(\overline{\mathfrak{g}}_i)^{-n}$, for each set of pairs $(\mathfrak{a}, \overline{\mathfrak{a}}) \in \mathcal{L}$. Define Λ_n to be a set of representatives of $U_{\mathbb{K}}/U_{\mathbb{K}}^n$. And finally define

$$\Gamma := \{\{\gamma u, \overline{\gamma u}\} : \{\gamma, \overline{\gamma}\} \in \Gamma', u \in \Lambda_n\}. \tag{2.16}$$

Therefore we have proved our theorem.

So our problem of determining the solutions of equation (2.2) turns into a problem of finding solutions of some Thue equations. We will not go through the theory of Thue equations, (for an account of that see [Coh07b, Chapter 12]) since we can use `MAGMA` ([BH96]), or even `pari/gp` (see [Han00]), to compute the solutions. We found `MAGMA` more suitable than `pari/gp` to solve the Thue equations that we will be looking at. Therefore using the result above and the facilities that `MAGMA` allows us to work with Algebraic number theory packages and solving Thue equations, a program was made to search for the solutions of (**LN**)

with D in our range (**R**). For $1 \leq D \leq 100$, the solutions of (**LN**) are given in the article [BMS06].

Now we will give a brief explanation why we consider the equation (2.2) instead of the equation (**GLRN**). While for the first one, we can factorize the left-hand side over the number field $\mathbb{Q}(\sqrt{-D})$, to factorize the second one we have to consider the number field $\mathbb{Q}(\sqrt{-D_2}, \sqrt{D_1})$, which can have at most degree 4 over $\mathbb{Q}$, implying at worst that it will have 3 fundamental units. As we will see having one fundamental unit will give us enough problems, now imagine what three could possibly do. Also in the latter case, instead of having Thue equations, we would have a curve defined by three homogenous polynomials of degree n, each one of 4 variables. So instead of solving an equation with two variables we would be finding points on a curve with four variables.

Now we will make some comments and observations about how to get the Thue equations and which ones we have to consider, after all.

2.2.1 Class Number

If $\mathfrak{O}_D$ has class number equal to 1, then we are working with a Principal Ideal Domain, so the construction of Γ is straightforward since we don't need to worry about inverses in the Class Group of our ideals $\mathfrak{a}_{\pm}$. On the other hand, if $\mathfrak{O}_D$ has class number greater than 1, we have to find our set Γ that has been defined above. Given $\{\gamma, \overline{\gamma}\} \in \Gamma$, we might not always have γ to be an algebraic integer. So the right hand sides of (2.5) and (2.6) might not be a polynomial in variables A and B with rational integers coefficients, but rational coefficients. As is known, given an algebraic number α, there exists $n \in \mathbb{N}$ such that $n\alpha$ is an algebraic integer. So given $\{\gamma, \overline{\gamma}\} \in \Gamma$, there exists n_γ, such that $n_\gamma\gamma$ is an algebraic integer, therefore seeing A, B as variables , we have that $n_\gamma\gamma(A+Bw)^m$ is a polynomial in variables

with rational integers coefficients as well its 'conjugate', $n_\gamma\overline{\gamma}(A+B\overline{\omega})^n$, and their sum too. Now instead of looking at the solutions of (2.6) we will look at the solutions of

$$2n_\gamma q = \frac{1}{\sqrt{d}}\Big(n_\gamma\overline{\gamma}(A+B\overline{\omega})^n - n_\gamma\gamma(A+B\omega)^n\Big).$$

A way to simplify the calculations is to find the 'minimal' γ, in terms of the norm, that we use to define the set Γ' as we did above. Let M_D be the Minkowski bound for the ring of integers $\mathfrak{O}_D$ and let $\mathcal{P}(M_D)$ be the set of ideals $\mathfrak{b}$ which norm is less or equal than the Minkowski bound M_D. Let $(\mathfrak{a},\overline{\mathfrak{a}}) \in \mathcal{L}$. Given $\mathfrak{c}_i$ a representative of the class group of $\mathfrak{O}_D$, such that $\mathfrak{a}{\mathfrak{c}_i}^{-m}$ is a principal ideal, consider the set $\mathfrak{I}_{\mathfrak{c}_i}(\mathfrak{a}) = \{\mathfrak{b} : \mathfrak{b} \in \mathcal{P}(\mathrm{M}_D),\ \mathfrak{b}{\mathfrak{c}_i}^{-1}$ is principal$\}$. Basically what we have done was to choose a representative at the same class of $\mathfrak{c}_i$ in the Class group, with norm less or equal to the Minkowski bound. Define $\mathfrak{G}(\mathfrak{a})$ to be the set containing one generator $\tilde{\gamma}$ of the principal ideals $\mathfrak{a}\mathfrak{b}^{-m}$, where $\mathfrak{b} \in \mathfrak{I}_{\mathfrak{c}_i}(\mathfrak{a})$, which is a finite set since $\mathfrak{I}_{\mathfrak{c}_i}$ is a finite set. So we can choose γ to be the element of $\mathfrak{G}(\mathfrak{a})$ which has the smallest norm.

While computing the Thue equations and their solutions, for the equation **LN**, we found that in most of cases, the only ideal $\mathfrak{a} \in \mathcal{L}$ we were getting was the trivial ideal $\mathfrak{O}_D$ so the corresponding class group member was itself and our γ was nothing more than 1. This can be explained, heuristically, by the fact that if there was an ideal $\mathfrak{a} \in \mathcal{L}$ different from the whole ring and a class group element $\mathfrak{c}_i$ such that $\mathfrak{a}{\mathfrak{c}_i}^{-m}$ was a principal ideal, a fractional one, but non-integral ideal, its generator would be an algebraic non-integer number lying inside ${\mathfrak{c}_i}^{-m}$ so we might end up with a huge denominator that would make the respective Thue equation almost impossible to solve.

2.2.2 $-D$ is a square

Suppose now $-D$ is a square, i.e., $-D = q^2$, so our field $\mathbb{K}_D$ is nothing more than $\mathbb{Q}$ and our ring of integers is then $\mathbb{Z}$. Instead of using the theory of ideals to compute the Thue equations we can use the unique factorization properties of the rational integers. Therefore we can rewrite our Theorem 2.1 in the following way,

Theorem 2.2. *Let D, q and n be as above and $R = \mathrm{Rad}(2q)^n$. If (x, y), with $y \neq 0$, is a solution to (2.2) then there exists natural numbers a, b, c_1 and c_2, such that:*

1. *$a \mid R$ and $b \mid R$,*
2. *if p is a prime then $p \mid a \Leftrightarrow p \mid b$,*
3. *ab is a perfect nth power*
4. *$c_1 c_2 = C$.*
5. *$x = \frac{1}{2}(bc_2U^n + ac_1V^n)$, where U, V are solutions of the following Thue equation:*

$$2q = (bc_2U^n - ac_1V^n).$$

Proof. Since $D = -q^2$, then we can rewrite (2.2) in the following way:

$$(x - q)(x + q) = Cy^n.$$

Since $y \neq 0$ we can use the unique factorization properties of $\mathbb{Z}$ to see that there exist numbers $a, b, c_1, c_2, y_1, y_2 \in \mathbb{Z}$, all different from 0, such that:

$$x - q = ac_1y_1^n, \quad x + q = bc_2y_2^n \quad \text{and } c_1c_2 = C.$$

We can always choose, without loss of generality, a, b to be natural numbers and for each prime p such that $p \mid a$ (resp. $p \mid b$) we can have that $p^n \nmid a$ (resp. $p^n \nmid b$).

Since $x^2 - q^2 = Cy^m$, and $c_1c_2 = C$ so we must have that $abc_1c_2(y_1y_2)^n = Cy^n$, therefore ab must be a perfect n-th power. By this fact and the fact that no n-th power of a prime divides both a and b, we must have that the primes that divides a are the same that divides b. So let us now consider p a prime such that $p|a$, we also have that $p|b$, so p divides both $x+q$ and $x-q$, therefore p divides $2q$. Thus we have that both a and b divides $(\mathrm{Rad}(2q))^n$. So we have a and b as in conditions (1)-(3) of the theorem. Of course (4) is already checked. To see condition (5), it is only necessary to see that $(x+q)-(x-q) = 2q$, on one side, while on the other side we get that $(x+q)-(x-q) = bc_2{y_2}^n - ac_1y_1^n$. So y_1, y_2 are solutions of the Thue equation $2q = (bc_2U^n - ac_1V^n)$. So we have that $x = \frac{1}{2}(bc_2U^n + ac_1V^n)$ and this concludes our proof. **QED**

Notice that we have imposed the condition $y \neq 0$ in the above theorem as in the others, but when $D = -q^2$, we also have the solution $(x, y) = (\pm q, 0)$, but this one might not arise from any of the Thue equations that we get using the above results. So in this particular case we have to consider this solution too.

2.2.3 Real and imaginary quadratic number fields

When $D < 0$, and $-D$ is not a square, $\mathbb{K}_D$ is a real quadratic number field. Its signature is $(r, s) = (2, 0)$ so the unit group $U_{\mathbb{K}_D}$ has rank 1, therefore there exists u a fundamental unit. Therefore we have that our set Λ_n is the following

$$\Lambda_n = \left\{ \pm 1, \pm u, \ldots, \pm u^{n-1} \right\}.$$

If n is odd then we can remove the $\pm$.

On the other hand when $D > 0$, we have that $\mathbb{K}_D$ is an imaginary quadratic number field. The signature is $(r, s) = (0, 1)$ and we know the unit group has

rank 0. Therefore $U_{\mathbb{K}_D}$ is equal to $\mu(\mathbb{K}_D)$. For this case we have that our set Λ_n is the following

$$\Lambda_n = \begin{cases} \{\pm 1\} & \text{if } d > 4 \text{ or } d = 2, \\ \{\pm 1, \pm i\} & \text{if } d = 1, \\ \{\pm 1, \pm\rho, \pm\rho\} & \text{if } d = 3, \end{cases}$$

where ρ is a primitive cube root of unity.

As before, if n is odd, then we can remove the "$\pm$".

2.2.4 Difference of squares

Consider now the particular case of $n = 2$ or an even number $2m$, for $m \in \mathbb{N}$. For this particular case we can consider the following equation

$$x^2 - Cy^2 = -D$$

instead of (2.2) and where the new y is equal to the old y to the power of m.

First of all these are the so called Pell-Fermat equations. If we consider the factorization of $x^2 - Cy^2$ over $\mathbb{K}_C = \mathbb{Q}(\sqrt{C})$, and C is not a square we have that $(x - y\sqrt{C})(x + y\sqrt{C}) = -D$, so $\mathcal{N}(x - y\sqrt{C}) = -D$, we are looking at norm equations.

As we have done before, we consider these factorizations (whether C is a square or not) as equations over ideals. Therefore we have that

$$\langle x - y\sqrt{C}\rangle\langle x + y\sqrt{C}\rangle = \langle -D\rangle.$$

So we need to look for ideals $\mathfrak{a}$ such that $\mathfrak{a}\overline{\mathfrak{a}} = \langle -D\rangle$ and $\mathfrak{a}$ and $\overline{\mathfrak{a}}$ are principal. Then there is $\gamma \in \mathfrak{O}_C$ the ring of integers of $\mathbb{K}_C$ such that $\mathfrak{a} = \langle\gamma\rangle$ and $\overline{\mathfrak{a}} = \langle\overline{\gamma}\rangle$. So $x = \frac{1}{2}(\gamma_u + \overline{\gamma}_u)$ and $y = \frac{1}{2\sqrt{C}}(\gamma_u - \overline{\gamma}_u)$, where u is a unit of $\mathfrak{O}_C$ and $\gamma_u = \gamma u$

So if $C < 0$ or a square we have that $U_{\mathbb{K}_C}$ is finite, so we will have finitely many solutions. The only problem arises when $\mathbb{K}_C$ is a real quadratic field, where there is a fundamental unit u_0 and so $u = \pm u_0^k$, where $k \in \mathbb{Z}$.

About the case when C is a square, let us say $C = c^2$, then the method to find the solutions becomes much easier. So $x + cy = d_1$ and $x - cy = d_2$, with d_1, d_2 integers such that $d_1 d_2 = -D$. And since we can choose x, y to be positive, we also have that $d_1 > 0$. And we see that $x = \frac{1}{2}(d_1 + d_2)$ and $y = \frac{1}{2c}(d_1 - d_2)$. So we have that $d_1 \equiv d_2 \pmod 2$ and $d_1 \equiv d_2 \pmod c$.

So we need to find all positive divisors d of $-D$ such that $d - D/d$ is even and $c \mid -D/d - d$.

2.3 Selmer groups and Γ sets

Though in the previous section we had mention how to obtain the Γ sets, we will now present another way of getting those sets. This method turns out to be more efficient in terms of computation, especially when we are computing also other information than factorizing ideals and/or finding their generators, as will happen in section 3.3.3. We will also show how we can shorten our set Γ, by eliminating some pairs $\{\gamma, \overline{\gamma}\}$ using local methods.

First some definitions and notation are needed before we carry on.

2.3.1 Selmer groups

We start presenting some definitions and stating some results concerning the so-called *Selmer groups* $Sel_n(\mathbb{K}, S)$, for a given integer n and a set S of finitely many primes ideals of the number field $\mathbb{K}$.

Definitions and main results

Definition 2.3.1. *Let $\mathbb{K}$ be a number field and $\mathbb{O}_{\mathbb{K}}$ its ring of integers. Let $Pl_f(\mathbb{K})$ the set of all the set of finite places of $\mathbb{K}$. Let S be a finite subset of $Pl_f(\mathbb{K})$, possibly empty, $\mathfrak{a}$ a fractional ideal of $\mathbb{O}$ and n a natural number greater than or equal to 2.*

(1) The ring of S-integers $\mathbb{O}_{\mathbb{K}}(S)$ is defined as

$$\mathbb{O}_{\mathbb{K}}(S) = \{x \in \mathbb{K} | v_{\mathfrak{p}}(x) \geq 0 \ \forall \mathfrak{p} \notin S\}$$

(2) We say that $\mathfrak{a}$ is coprime with S if $v_{\mathfrak{p}}(\mathfrak{a}) = 0$, for all ideals $\mathfrak{p} \in S$.

(3) We say that $\mathfrak{a}$ is an S-ideal if it belongs to the group of (fractional) ideals generated by ideals in S, that is, $v_{\mathfrak{p}}(\mathfrak{a}) = 0$ for all ideals $\mathfrak{p} \in Pl_f(\mathbb{K}) \setminus S$. The set of all S-ideals will be denoted by $\mathcal{I}_{\mathbb{K}}(S)$.

(4) We say that an element $u \in \mathbb{K}^*$ is an S-unit if $v_{\mathfrak{p}}(u) = 0$ for every prime ideal $\mathfrak{p} \in Pl_f(\mathbb{K}) \setminus S$. The group of S-units is denoted by $U_{\mathbb{K}}(S)$.

(5) We define the S-class group $Cl_{\mathbb{K}}(S)$ as the quotient group of the ordinary class group $Cl_{\mathbb{K}}$ by the subgroup generated by the classes of the elements of S.

(6) We say that an element $u \in \mathbb{K}^*$ is an S-virtual n-th power if $v_{\mathfrak{p}}(u) \equiv 0 \pmod{n}$ for every prime ideal $\mathfrak{p} \in Pl_f(\mathbb{K}) \setminus S$.

(7) We define the n-Selmer group of $\mathbb{K}$ with respect to S, $Sel_n(\mathbb{K}, S)$ as the set of classes of S-virtual n-th powers modulo $\mathbb{K}^{*n}$.

Given S as in the definition and an ideal $\mathfrak{a}$ of $\mathbb{O}$, integral or not, we know, by the fundamental theorem of ideals, that $\mathfrak{a} = \prod_{\mathfrak{p} \in Pl_f(\mathbb{K})} \mathfrak{p}^{m_{\mathfrak{p}}}$, where $m_{\mathfrak{p}}$ is an

integer equal to zero, except for finitely many prime ideals $\mathfrak{p}$. We denoted by $\mathfrak{a}_S = \prod_{\mathfrak{p}\in S} \mathfrak{p}^{m_\mathfrak{p}}$ and by $\mathfrak{a}_{\overline{S}} = \prod_{\mathfrak{p}\in Pl_f(\mathbb{K})\setminus S} \mathfrak{p}^{m_\mathfrak{p}}$. Therefore we have that $\mathfrak{a} = \mathfrak{a}_S\mathfrak{a}_{\overline{S}}$, where $\mathfrak{a}_S$ is an S-ideal and $\mathfrak{a}_{\overline{S}}$ is an ideal coprime with S.

Now we give two results that will help us work with the n-Selmer group of our number field $\mathbb{K}_D$ for a given finite set of prime ideals S.

Proposition 2.3.1. *Let S and n be as in the definition above. The following two properties are equivalent.*

(1) u is an S-virtual n-th power.

(2) There exist (fractional) ideals $\mathfrak{a}, \mathfrak{b}$ of $\mathbb{O}$ such that:

$$\langle u\rangle = \mathfrak{a}\mathfrak{b}^n,$$

where $\mathfrak{b}$ is coprime to S and $\mathfrak{a}$ is an S-ideal.

Proof. That (2) implies (1) is trivial. About (1) implying (2), consider the ideal $\mathfrak{u} = \langle u\rangle$, by the definition of S-virtual n-th power and $v_\mathfrak{p}(u) = 0$ for all ideals $\mathfrak{p} \in Pl_f(\mathbb{K}) \setminus S$, so $v_\mathfrak{p}(\langle u\rangle) = v_\mathfrak{p}(u) = 0$ for all ideals $\mathfrak{p} \in Pl_f(\mathbb{K}) \setminus S$. By the observation made above, we have that $\mathfrak{u} = \mathfrak{u}_S\mathfrak{u}_{\overline{S}}$, where $\mathfrak{u}_{\overline{S}}$ is a n-th power,by hypothesis, so $\mathfrak{u}_{\overline{S}} = \mathfrak{b}^n$. Therefore we have $\langle u\rangle = \mathfrak{u}_S\mathfrak{b}^n$ where $\mathfrak{b}$ is coprime to S, since $\mathfrak{b}^n = \mathfrak{u}_{\overline{S}}$, that is coprime to S. **QED**

The following result can be found in [CL07]. Even so we do not refrain from presenting a proof.

Proposition 2.3.2. *Let S be as in the previous proposition and m and n coprime natural numbers. Then $Sel_{mn}(\mathbb{K}, S) \simeq Sel_m(\mathbb{K}, S) \times Sel_n(\mathbb{K}, S)$.*

Proof. First of all, since m and n are coprime there are $k_1, k_2 \in \mathbb{Z}$ such that $mk_1 + nk_2 = 1$. Now we define two monomorphisms ϕ_1, ϕ_2; the first from $Sel_{mn}(\mathbb{K}, S)$

to $Sel_m(\mathbb{K},S)\times Sel_n(\mathbb{K},S)$ and the second one in the opposite direction. Given $[a]\in Sel_{mn}(\mathbb{K},S)$ we set $\phi_1([a])=([a],[a])$ and given $([a],[b])\in Sel_m(\mathbb{K},S)\times Sel_n(\mathbb{K},S)$, we set $\phi_2(([a],[b]))=[a^{nk_2}b^{mk_1}]$. First of all it is easy to see that ϕ_1 is well defined, since if $[a]=[b]\in Sel_{mn}(\mathbb{K},S)$ it is equivalent to say that $a=b\alpha^{mn}$, with both a and b S-virtual mn-powers, and $\alpha\in\mathbb{K}^*$, which is equivalent to $[a]=[b]$ in both $Sel_m(\mathbb{K},S)$ and $Sel_n(\mathbb{K},S)$. It is easy to see that ϕ_2 is well defined.

Let $([a],[b])\in Sel_m(\mathbb{K},S)\times Sel_n(\mathbb{K},S)$. We have that $\phi_2([a],[b])=[a^{nk_2}b^{mk_1}]$. Now

$$a^{nk_2}b^{mk_1}=a^{1-mk_1}b^{mk_1}=a(a^{-1}b)^{mk_1}.$$

So $[a^{1-mk_1}b^{1-nk_2}]=[a]$ in $Sel_m(\mathbb{K},S)$. The same is also true for $[a^{1-mk_1}b^{1-nk_2}]=[b]$ in $Sel_n(\mathbb{K},S)$. So $\phi_1\circ\phi_2=Id_{m\times n}$. It is also easy to prove that $\phi_2\circ\phi_1=Id_{mn}$. **QED**

Proposition 2.3.3. *Let $\mathbb{K}$ be a number field of signature (r,s), S as above. We denote by $\#S$ the cardinality of S. Define $\kappa(S)=r+s+\#S-1$. Let $\mu(\mathbb{K})$ be the torsion subgroup of $U_{\mathbb{K}}$. Let p be a prime number and l an integer greater than or equal to 0. Define r_l to be the non-negative integer such that $\gcd(p^l,\#\mu(\mathbb{K}))=p^{r_l}$.*

(1) The group $U_{\mathbb{K}}(S)$ is a finitely generated abelian group of rank $\kappa(S)$, whose torsion subgroup is independent of S and equal to the (cyclic) group of roots of unity of $\mathbb{K}$. In particular,

$$\left|\frac{U_{\mathbb{K}}(S)}{U_{\mathbb{K}}(S)^{p^l}}\right|=p^{l\kappa(S)+r_l}.$$

(2) We have a natural split exact sequence

$$1\longrightarrow\frac{U_{\mathbb{K}}(S)}{U_{\mathbb{K}}(S)^{p^l}}\longrightarrow Sel_{p^l}(\mathbb{K},S)\longrightarrow Cl_{\mathbb{K}}(S)[p^l]\longrightarrow 1, \tag{2.17}$$

where as usual for an abelian group G, $G[p^l]$ denotes the subgroup of G killed by p^l. In particular, $Sel_{p^l}(\mathbb{K}, S)$ is finite and its cardinality is equal to $p^{\kappa(S)+r_l+c_l}$, where c_l is the integer such that $\#Cl_{\mathbb{K}}(S)[p^l] = p^{c_l}$.

Proof. The proof that is largely based on the proof of Proposition 8.3.4 of [Coh07b]

(1). We have a natural sequence

$$1 \longrightarrow U_{\mathbb{K}} \longrightarrow U_{\mathbb{K}}(S) \longrightarrow \mathcal{I}_{\mathbb{K}}(S) \longrightarrow Cl_{\mathbb{K}} \longrightarrow Cl_{\mathbb{K}}(S) \longrightarrow 1,$$

where the map starting from $U_{\mathbb{K}}(S)$ sends u to the Ideal $\langle u \rangle$, and the map starting from $\mathcal{I}_{\mathbb{K}}(S)$ sends an ideal to its ideal class. It is immediately checked that the sequence is indeed exact. Since $Cl_{\mathbb{K}}$ and, therefore also, $Cl_{\mathbb{K}}(S)$ are finite groups, it follows that $U_{\mathbb{K}}(S)$ is finitely generated and its rank is equal to that of $U_{\mathbb{K}}$, $(r_1 + r_2 - 1)$ plus that of $\mathcal{I}_{\mathbb{K}}(S)$, equal to $\#S$, that is, the rank is equal to $\kappa(S)$. The statement concerning the torsion subgroup is clear, and the one about the order of the quotient group $U_{\mathbb{K}}(S)/U_{\mathbb{K}}(S)^{p^l}$ is also clear, taking into account the order of the torsion subgroup.

(2). Let $\overline{u} \in Sel_{p^l}(\mathbb{K}, S)$, so that $\langle u \rangle = \mathfrak{a}\mathfrak{b}^{p^l}$, for some S-ideal $\mathfrak{a}$, from what we have seen from the proposition above. We send $\overline{u}$ to the class of $\mathfrak{b}$ in $Cl_{\mathbb{K}}(S)$. Clearly this does not depend on the decomposition $\mathfrak{a}\mathfrak{b}^{p^l}$, which is unique, or on the chosen representative u of $\overline{u} \in Sel_{p^l}(\mathbb{K}, S)$. Since $\mathfrak{b}^{p^l} = u\mathfrak{a}^{-1}$ it is clear that the class of $\mathfrak{b}$ belongs in fact to $Cl_{\mathbb{K}}(S)[p^l]$. With this map defined, it is then easily checked that the given sequence is exact and split. The statements concerning the cardinality of $Sel_{p^l}(\mathbb{K}, S)$ follow. **QED**

We have used the basic exact sequence (2.17), called the p^l-Kummer sequence for $\mathbb{K}^*$ (or for $U_{\mathbb{K}}(S)$). In fact this sequence is more general than presented

in (2.17): for a given positive integer n we have:

$$1 \longrightarrow \frac{U_{\mathbb{K}}(S)}{U_{\mathbb{K}}(S)^n} \xrightarrow{\iota_n} Sel_n(\mathbb{K}, S) \xrightarrow{\alpha_n} Cl_{\mathbb{K}}(S)[n] \longrightarrow 1$$

where $Cl_{\mathbb{K}}(S)[n]$ is the n-torsion subgroup of $Cl_{\mathbb{K}}(S)$, and the map α_n is given by $x \mapsto [\mathfrak{b}]$, where $\langle x \rangle = \mathfrak{a}\mathfrak{b}_S^n$, with $\mathfrak{a}$ an S-ideal and $\mathfrak{b}$ a coprime S-ideal

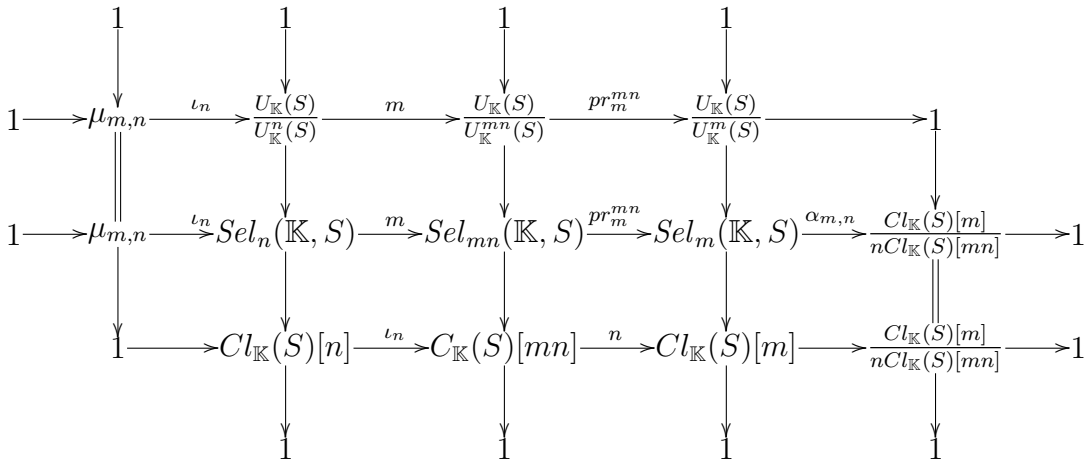
There is an analogy with the n-descent Kummer sequence for elliptic curves,

$$0 \longrightarrow E(\mathbb{K})/nE(\mathbb{K}) \longrightarrow Sel^{(n)}(\mathbb{K}, E) \longrightarrow Ш[m] \longrightarrow 1.$$

Let us present two ways of calculating $Sel_n(\mathbb{K}, S)$ for a given positive integer and S, a finite set of prime ideals.

The first result is presented, once again, in [CL07].

Proposition 2.3.4. *Let m, n be positive integers. The Kummer sequences for m, mn and n fit together to form the following commutative diagram with exact rows and columns:*



The kernels $\mu_{m,n} = \mu_m(\mathbb{K})/\mu_{mn}(\mathbb{K})^n$ are finite, and trivial when $\gcd(m, n) = 1$. The cokernels $Cl_{\mathbb{K}}[S][m]/nCl_{\mathbb{K}}(S)[mn]$ are also finite, and also trivial when $\gcd(m, n) = 1$ or when $\#Cl_{\mathbb{K}}(S)$ is coprime to m.

Proof. We provide a proof for this result. The columns are exact due to the Kummer sequence for the central columns and due to the trivial maps for the external columns. About the rows, let us start by the first one. Let $u \in U_{\mathbb{K}}(S)$, such that $[u^m] \in U_{\mathbb{K}}^{mn}(S)$, then exists $v \in U_{\mathbb{K}}(S)$, such that $u^m = v^{nm}$, therefore $u = \zeta v^n$, where $\zeta \in \mu_{m,n}$. So the sequence is exact at $U_{\mathbb{K}}(S)/U_{\mathbb{K}}^n(S)$. About the exactness in $U_{\mathbb{K}}(S)/U_{\mathbb{K}}^{mn}(S)$. Let $u \in U_{\mathbb{K}}(S)$, then $u \in U_{\mathbb{K}}^m(S)$, if and only if $u = v^m$, therefore u belongs to the image of m. And it is clear that the image of pr_m^{mn} is the whole group $U_{\mathbb{K}}(S)/U_{\mathbb{K}}^m(S)$.

For the second row. Let $[u] \in Sel_n(\mathbb{K}, S)$ such that $[u^m]$ is trivial in $Sel_{mn}(\mathbb{K}, S)$, then $u^m = v^{mn}$, therefore as before we have that $u = v^n\zeta$, with $\zeta \in \mu_{m,n}$. If $[u] \in Sel_{mn}(\mathbb{K}, S)$ is trivial in $Sel_m(\mathbb{K}, S)$, then $u = v^m$, and since $u \in Sel_{mn}(\mathbb{K}, S)$ we have that $[v] \in Sel_n(\mathbb{K}, S)$. And it's clear that the image of m belongs to the kernel. Now let $[u]$ belong to the kernel of $\alpha_{m,n}$, then $\langle u \rangle = \mathfrak{a}_S\mathfrak{b}_{\overline{S}}^m$ and $[\mathfrak{b}_{\overline{S}}] = [\mathfrak{c}^n]$, with $[\mathfrak{c}] \in Cl_{\mathbb{K}}(S)$. Therefore we can see that $\langle u \rangle = \tilde{\mathfrak{a}}\tilde{\mathfrak{c}}^{mn}$, that is $[u] \in Sel_{mn}(\mathbb{K}, S)$. It is also easy to see that $\alpha_{m,n}$ is surjective. For the last row we just need to check that $\ker n = \operatorname{im} \iota_n$. Consider $[\mathfrak{a}] \in \ker n$, then $[\mathfrak{a}^n] = [\mathfrak{c}]$, with $\mathfrak{c}$ and S-ideal. Then $[\mathfrak{a}] \in Cl_{\mathbb{K}}(S)[n]$. The other inclusion is obvious. About the commutativity of the diagram, this is obvious by the definition of the maps and taking into account that if $u \in U_{\mathbb{K}}(S)$, then $\alpha_m([u])$ is always the trivial element. **QED**

With this result we can compute $Sel_n(\mathbb{K}, S)$ in the following way. First we factorize n into a product of prime powers $n = p_1^{m_1} \dots p_r^{m_r}$ and then we calculate separately each $Sel_{p_i^{m_i}}(\mathbb{K}, S)$. Let p be a prime dividing n, and $\kappa_p = v_p(n)$To start we need to calculate $Sel_p(\mathbb{K}, S)$, which can be done by our `MAGMA` implementation. Suppose we have calculated $Sel_{p^r}(\mathbb{K}, S)$, next we calculate $Sel_{p^{r+1}(\mathbb{K},S)}$. First we

determine the homomorphism $\alpha_{p,p^r} : Sel_p(\mathbb{K}, S) \to Cl_{\mathbb{K}}(S)[p]/p^r Cl_{\mathbb{K}}(S)[p^{r+1}]$: for each $u \in Sel_p(\mathbb{K}, S)$ we may write $\langle u \rangle = a_S b_S^p$ and set $\alpha(u)$ to be the class of b_S modulo $Cl_{\mathbb{K}}(S)[p^{r+1}]$. If $[b_S] = I_S^{p^r}$, for some co-prime S-ideal I_S, then writing $vb_S = I_S^{p^r}$, with $v \in \mathbb{K}^*$ we can replace u by uv^p, which represents the same class in $Sel_p(\mathbb{K}, S)$ as u. Thus for each generator of the kernel of α_{p,p^r} we can lift to a representative element $u \in \mathbb{K}^*$ such that u modulo $(\mathbb{K}^*)^{p^{r+1}}$ lies in $Sel_{p^{r+1}}(\mathbb{K}, S)$. Then $Sel_{p^{r+1}}(\mathbb{K}, S)$ is generated by these elements together with the v^p for v in a set of generators of $Sel_{p^r}(\mathbb{K}, S)$ modulo $\iota_p(\mu_{p,p^r})$. And we proceed like this until we calculate $Sel_{p^{\kappa_p}}(\mathbb{K}, S)$.

The problem with this method is that it depends on constructing almost every single Selmer group for each prime power dividing n. We need to calculate every single Selmer group from p to $p^{\kappa_p/}$. There is a more steady way of calculating our Selmer group without going through a recursive process.

Theorem 2.3. *Let S be a finite set of prime ideals of $\mathbb{K}$, n a positive integer. Let S' be a finite set, possibly empty, of prime ideals of $\mathbb{K}$ such that $S \cap S' = \emptyset$ and the representatives of the elements of $S^* := S \cup S'$ generates the group $Cl_{\mathbb{K}}/nCl_{\mathbb{K}}$. Define $\mathbb{K}_n(S, S') := \{u \in U_{\mathbb{K}}(S^*) : v_{\mathfrak{p}}(u) \equiv 0 \pmod{n}, \forall \mathfrak{p} \in S'\}$. Then*

$$\mathbb{K}_n(S, S')/(\mathbb{K}_n(S, S'))^n \simeq Sel_n(\mathbb{K}, S).$$

Proof. The existence of S^* is due to the fact that $Cl_{\mathbb{K}}$ is finite and hence so is $Cl_{\mathbb{K}}/nCl_{\mathbb{K}}$. Using a method similar to the one described in 2.2.1 to find a set of representatives for each class of $Cl_{\mathbb{K}}$, we can build a finite set S', possibly empty, such that $S' \cap S = \emptyset$ and $S^* = S \cup S'$ generates $Cl_{\mathbb{K}}/nCl_{\mathbb{K}}$. Let $u \in \mathbb{K}_n(S, S')$, we define the map $\phi^n_{S,S'}$, from $\mathbb{K}_n(S^*)/\mathbb{K}_n^n(S, S')$ to $Sel_n(\mathbb{K}, S)$ in the following way, $\phi^n_{S,S'}([u]) = [u]$. Let us see that is well defined. Let $u \in \mathbb{K}_n(S, S')$ so for all $\mathfrak{p}$ prime ideals of $\mathbb{K}$ outside S^*, we have that $v_{\mathfrak{p}}(u) = 0$ and, due to the

definition of $\mathbb{K}_n(S,S')$, we have that $v_{\mathfrak{p}}(u) \equiv 0 \pmod{n}$, when $\mathfrak{p} \in S'$, therefore $[u] \in Sel_n(\mathbb{K},S)$. Now let $v \in \mathbb{K}_n(S,S')$. First assume that $[u]=[v]$, thus there exists $w \in \mathbb{K}_n(S,S')$ such that $u = vw^n$, therefore $[u]=[v]$ in $Sel_n(\mathbb{K},S)$. Suppose now we have $\phi^n_{S,S'}([u]) = \phi^n_{S,S'}([v])$, then exists $b \in \mathbb{K}^*$, such that $u = vb^n$, therefore for all prime ideals $\mathfrak{p}$ we have that $v_{\mathfrak{p}}(u) = v_{\mathfrak{p}}(v) + nv_{\mathfrak{p}}(b)$, and since $u, v \in \mathbb{K}_n(S,S')$, we see that $v_{\mathfrak{p}}(b) = 0$ for all prime ideals $\mathfrak{p}$ not in S^*, therefore $[u]=[v]$ in $\mathbb{K}_n(S,S')/\mathbb{K}^n_n(S,S')$. This proves that $\phi^n_{S,S'}$ is injective. Now let us prove that $\phi^n_{S,S'}$ is surjective. Let $[u] \in Sel_n(\mathbb{K},S)$, then we know that $\langle u \rangle = \mathfrak{a}\mathfrak{b}^n$, with $\mathfrak{a}$ an S-ideal and $\mathfrak{b}$ an S-coprime ideal. So we have that $\mathfrak{b} \in Cl_{\mathbb{K}}(S)[n]$. Due to the fact that S^* generates $Cl_{\mathbb{K}}/nCl_{\mathbb{K}}$, we have that $[\mathfrak{b}]^{-1} = [\mathfrak{c}]$, with $\mathfrak{c}$ an S^*-ideal. Therefore $\mathfrak{b}\mathfrak{c} = \langle c_u \rangle$ and we have that

$$\langle u \rangle = \mathfrak{a}\mathfrak{b}^n = \mathfrak{a}\mathfrak{b}^n\mathfrak{c}^n\mathfrak{c}^{-n} = c_u^n\mathfrak{a}\mathfrak{c}^n.$$

So consider uc_u^{-n}. This element is in $\mathbb{K}_n(S,S')$, since $v_{\mathfrak{p}}(uc_u^{-n}) = v_{\mathfrak{p}}(\mathfrak{a}\mathfrak{c}^{-n})$, $\mathfrak{a}$ is an S-ideal and $\mathfrak{c}$ an S^*-ideal and $\phi^n_{S,S'}([uc_u^{-n}]) = [u]$. Now we have to see that it does not depend on our choice of $\mathfrak{c}$. Suppose that there is another S^*-ideal $\mathfrak{d}$, such that $\langle u \rangle = \tilde{c}^n\mathfrak{a}\mathfrak{d}^{-n}$, then consider $w = \left(\frac{c_u}{\tilde{c}}\right)^n$. We have that $v_{\mathfrak{p}}(w) = n(v_{\mathfrak{p}}(\mathfrak{c}) - v_{\mathfrak{p}}(\mathfrak{d}))$, therefore we have that $w \in \mathbb{K}^n_n(S,S')$, and so uc_u^{-n} and ud^{-n} are in the same class in $\mathbb{K}_n(S,S')/\mathbb{K}^n_n(S,S')$. Also suppose that u, v are such that $[u]=[v] \in Sel_n(\mathbb{K},S)$, then exists c_u, c_v as before and $w \in \mathbb{K}^*$ such that $u = vw^n$. So $uc_u^{-n}/vc_v^{-n} = vw^nc_u^{-n}/vv_v^{-n} = (wc_v/c_u)^n$, and is easy to see that wc_v/c_u is in $\mathbb{K}_n(S,S')$, just consider as before the ideal representation of uc_u^{-n} and vc_v^{-n}. And for course we have that $\phi^n_{S,S'}([uc_u^{-n}]) = [uc_u^{-n}] = [u]$. Therefore we have that $\mathbb{K}_n(S,S')/\mathbb{K}^n_n(S,S') \simeq Sel_n(\mathbb{K},S)$. **QED**

It is possible to implement an algorithm in `MAGMA` to compute the $Sel_n(\mathbb{K},S)$, for a given positive integer n, a number field $\mathbb{K}$ and S a finite set of primes ideals

of $\mathbb{K}$.

Constructing the Γ sets using Selmer groups

Consider $\{\gamma, \overline{\gamma}\} \in \Gamma'$. Consider $S(2DC)$ to be set of the prime ideals dividing the ideal $\langle 2DC \rangle$. By the definition of γ, we have that if $(\alpha, \overline{\alpha}) \in \Gamma'$, then $\langle \alpha \rangle = \mathfrak{a}\mathfrak{b}^n$; it is possible to choose $\mathfrak{b}$ and $\mathfrak{a}$ such that $\mathfrak{a}$ is an $S(2DC)$-ideal and $\mathfrak{b}$ is coprime to $S(2DC)$. So we have that α is an $S(2DC)$-virtual n-th power. From now on set $S := S(2DC)$. Now, let $\{\gamma, \overline{\gamma}\}, \{\gamma', \overline{\gamma}'\} \in \Gamma'$ and suppose that they define the same class in n-Selmer group of $\mathbb{K}_D$ with respect to S. So $\gamma = \gamma' u^n$, where $u \in \mathbb{K}_D^*$, therefore

$$\langle \gamma \rangle = \langle \gamma' u^n \rangle. \tag{2.18}$$

By the definition of γ and γ' we have that there exists $\mathfrak{a}_1, \mathfrak{a}_2, \mathfrak{c}_1, \mathfrak{c}_2$ such that

$$\langle \gamma \rangle = \mathfrak{a}_1 \mathfrak{c}_1^n \quad \text{and} \quad \langle \gamma' \rangle = \mathfrak{a}_2 \mathfrak{c}_2^n, \tag{2.19}$$

with $\mathfrak{a}_1$ and $\mathfrak{a}_2$ S-ideals such that $0 \leq v_{\mathfrak{p}}(\mathfrak{a}_i) \leq n-1$, for all $\mathfrak{p} \in S$ and $i \in \{1, 2\}$.

So joining the information of (2.18) and (2.19) we have that:

$$\mathfrak{a}_1 \mathfrak{c}_1^p = \mathfrak{a}_2 (u\mathfrak{c}_2)^n.$$

So by the definition of $\mathfrak{a}_i$, we have that $\mathfrak{a}_1 = \mathfrak{a}_2$, and therefore $\mathfrak{c}_1 = u\mathfrak{c}_2$, but since each $\mathfrak{c}_i$ was chosen as a representative of a class of the class group of $\mathbb{K}_D$, and $\mathfrak{c}_2$ and $u\mathfrak{c}_2$ are in the same class we have that $\mathfrak{c}_1 = \mathfrak{c}_2$, therefore $\gamma = \gamma'$, by the definition of Γ'.

This means that instead of creating the S ideals $\mathfrak{a}$ nth power free and going through the tedious process of seeing if it is principal or not, and then finding a suitable γ, we can look directly to representatives of the n-Selmer group of $\mathbb{K}_D$ with respect to S. Of course there are still more properties that we need to verify. Recall $\mathcal{L}$ as defined above, $(\mathfrak{a}, \overline{\mathfrak{a}}) \in \mathcal{L}$, had to verify three conditions:

(i) $0 \leq v_{\mathfrak{p}}(\mathfrak{a}) < n$ for $\mathfrak{p} \in S$ and $v_{\mathfrak{p}}(\mathfrak{a}) = 0$ if $\mathfrak{p} \notin S$.

(ii) the $\gcd(\mathfrak{a}, \overline{\mathfrak{a}})$ divides $(2q\sqrt{-d})\mathfrak{O}_D$;

(iii) $v_l(\mathcal{N}(\mathfrak{a})) \equiv v_l(C) \pmod{n}$ for l dividing C and $v_{\mathfrak{p}}(\mathfrak{a}\overline{\mathfrak{a}}) \equiv 0 \pmod{n}$ for all $\mathfrak{p} \in S(2D \setminus C)$.

So we need to see how we should get representatives of the Selmer group that satisfy the two last conditions.

For $\mathfrak{a}\overline{\mathfrak{a}}$ to be an n-th power, the norm of $\mathfrak{a}$ must be an n-th power, so by the choice of $\{\gamma, \overline{\gamma}\} \in \Gamma'$, we have that the valuation of γ is a multiple of n for the primes in $S(2D \setminus C)$. Then we have to look for representatives of the n-Selmer group whose valuation is a multiple of n for the primes in $S(2D \setminus C)$. By the definition of S-virtual n-th power, we only need to look at what happens with the powers of the primes that divide $2D$ but do not divide C, in the norm of the representatives of the n-Selmer group. Let q be a prime dividing $2D$ but not C. Consider the map

$$\theta_q : Sel_n(\mathbb{K}_D, S) \to \mathbb{Z}/n\mathbb{Z},$$

defined by $\theta_q(\overline{u}) = (v_q(\mathcal{N}(u)) \pmod{n})$. By condition (iii) above, we have that $\gamma \in Ker(\theta_q)$, for all primes $q \mid 2D$ and $q \nmid C$. The second part of third condition is settled so let us consider the first part. We must have $\mathcal{N}(\mathfrak{a})/C$ an nth power. Let l be a prime diving C. Define then the map

$$\psi_l : Sel_n(\mathbb{K}_D, S) \to \mathbb{Z}/n\mathbb{Z},$$

defined by $\psi_l(\overline{u}) = v_l(\mathcal{N}(u)) \pmod{n}$. Again by condition (iii), we have that $\{\gamma, \overline{\gamma}\} \in \Gamma'$ only if $\gamma \in \phi_l^{-1}(v_l(C) \pmod{n})$.

This takes care of the third condition.

Let us now consider the second condition, (ii), $\gcd(\mathfrak{a}, \overline{\mathfrak{a}})$ divides $2q\sqrt{d}\mathfrak{D}_D$. If $\{\gamma, \overline{\gamma}\} \in \Gamma'$, then there exists $(\mathfrak{a}, \overline{\mathfrak{a}}) \in \mathcal{L}$ and a fractional ideal $\mathfrak{c}$ such that

$$\langle \gamma \rangle = \mathfrak{a}\mathfrak{c}^{-n}.$$

As we have seen before, we have that $\mathfrak{a}$ is an S-ideal.

So, given a γ representative of a class of $Sel_n(\mathbb{K}, S)$, we have that

$$\langle \gamma \rangle = \prod_{i=1}^{m} \mathfrak{p}_i^{k_i},$$

with $\mathfrak{p}_i$ prime ideals and k_i nonzero integers.

Define then $\langle \gamma \rangle_{S,n}$ to be the following ideal:

$$\langle \gamma \rangle_{S,n} := \prod_{i=1}^{r} \mathfrak{p}_i^{\kappa_i},$$

where $\kappa_i = k_i$ if $k_i > 0$ or $\kappa_i \equiv k_i \pmod{n}$, with $\kappa_i \in \{0, 1, \ldots, n-1\}$. Then we have that $\langle \gamma \rangle_{S,n}$ is an S ideal and

$$\langle \gamma \rangle = \langle \gamma \rangle_{S,n} \mathfrak{c}_{S,n}^{-n}.$$

So to have $\{\gamma, \overline{\gamma}\} \in \Gamma'$, we must have that $\gcd(\langle \gamma \rangle_{S,n}, \langle \overline{\gamma} \rangle_{S,n})$ divides $2q\sqrt{-d}$.

In conclusion we have proved the following result:

Theorem 2.4. *Keeping the notation above we have that $\{\gamma, \gamma'\} \in \Gamma'$ if it satisfies the following conditions:*

(1) γ is an S-virtual n-th power.

(2) $\gcd(\langle \gamma \rangle_{S,n}, \langle \overline{\gamma} \rangle_{S,n}) \mid 2q\sqrt{-d}$.

(3)

$$[\gamma] \in \bigcap_{l \mid 2DC} \psi_l^{-1}(v_l(C) \pmod{n}),$$

where $[\gamma]$ is the class of γ in the $Sel_n(\mathbb{K}_D, S)$, and q and l are prime numbers.

(4) If $(\alpha, \overline{\alpha}) \in \Gamma'$ different from $\{\gamma, \overline{\gamma}\}$, satisfies the above conditions then

$$\langle \alpha \rangle_{S,n} \neq \langle \gamma \rangle_{S,n} \text{ and } \langle \overline{\alpha} \rangle_{S,n} \neq \langle \gamma \rangle_{S,n}.$$

Though we have shown that distinct $\{\gamma, \overline{\gamma}\}, \{\gamma', \overline{\gamma}'\} \in \Gamma'$ come from different n-Selmer groups class, the opposite is not true, in fact we can have that two different n-Selmer class verifying the conditions above can give rise to two elements that come from some ideal $\mathfrak{a} \in \mathfrak{L}$. This is due to the fact of for different classes of the Selmer group $[\gamma]$ and $[\gamma']$, we can have $\langle \gamma \rangle_{S,n} = \langle \gamma' \rangle_{S,n}$ or $\langle \overline{\gamma} \rangle_{S,n} = \langle \gamma' \rangle_{S,n}$. That's the reason to impose the condition (4).

With this result, instead of creating the set of ideals $\mathcal{L}$ and then testing all the conditions for each of those ideals, we can create first the set of n-Selmer group of $\mathbb{K}_D$ with respect to the set S, defined above and then verify conditions (2), (3) and (4) of the previous theorem.

As before, it is possible to obtain the n-Selmer group for the field $\mathbb{K}_D$ with respect to $S(2DC)$, using the program `MAGMA`. As it also possible to implement computational routines to verify condition (2), (3) and (4). Apart from the advantage of not having to create the set $\mathcal{L}$, we also don't need to test if each ideal is principal and, if not, choose a representative for the inverse class in the class group. A possible disadvantage of this method, seems to appear when we have the field $\mathbb{K}_D$ with class number one and we get some of the γ non-integral, due to the fact that the choice of a representative of a class of $Sel_n(\mathbb{K}_D, S)$ group can be an algebraic number that is not necessarily an algebraic integer.

2.3.2 Sieving Γ

After obtaining Γ' we still have to build the set Γ as shown in (2.16). Now we will present a method that might, or not, eliminate some of the elements of Γ

that we do not need to consider for our Thue equations. This method has been used before in [BMS06] to help eliminate modular forms or to find the $\{\gamma, \overline{\gamma}\}$ that would give rise to a Thue equation. We will use it later on with modular forms, but we will present now an adaptation of that method.

Suppose that l is a prime satisfying the following conditions.

(a) $l \nmid 2D$.

(b) $l = nm + 1$ for some integer m.

(c) $(\frac{-d}{l}) = 1$, thus l splits in $\mathfrak{O}_D$, say $(l) = \mathfrak{l}_1\mathfrak{l}_2$.

(d) Each $\gamma \in \Gamma$ is integral at l; what we mean by this is that each γ belongs to the intersection of the localizations $\mathfrak{O}_{D,\mathfrak{l}_1} \cap \mathfrak{O}_{D,\mathfrak{l}_2}$.

For such prime l we define $\mathcal{I}_l(D)$ to be the set of $\tau \in \mathbb{F}_l$ such that either:

- $(\tau^2 + D)^m \equiv C^m \pmod{l}$; or
- $(\tau^2 + D)^m \equiv 0 \pmod{l}$,

where m is as above.

We denote the two natural reduction maps by $\theta_1, \theta_2 : \mathfrak{O}_{D,\mathfrak{l}_1} \cap \mathfrak{O}_{D,\mathfrak{l}_2} \to \mathbb{F}_l$. These of course correspond to the two square roots for d in $\mathbb{F}_l$ and are easy to compute.

Now let Γ_l be the set of $\gamma \in \Gamma$ for which there exists $\tau \in \mathcal{I}_l(D)$ such that:

- $(\tau + q\theta_1(\sqrt{-d}))^m \equiv \theta_1(\gamma)^m$ or $0 \pmod{l}$; and
- $(\tau + q\theta_2(\sqrt{-d}))^m \equiv \theta_2(\gamma)^m$ or $0 \pmod{l}$.

Proposition 2.3.5. *Let D and C be as before. Let $T(n)$ be a set of primes l satisfying the conditions (a)-(d) above. With the notation as above, if there is*

Table 2.1: Number of Thue equations we must consider for Γ and for Γ_T

		D											
n	Γ or Γ_T	-11	-17	-19	-33	-38	-53	-56	-62	-66	-71	-77	-86
3	Γ	3	9	3	9	3	3	3	3	3	3	3	3
	Γ_T	2	6	3	6	3	0	3	3	3	3	3	3
5	Γ	5	15	5	15	5	5	5	5	5	5	5	5
	Γ_T	5	10	0	8	4	2	2	5	0	4	5	0
7	Γ	7	21	7	21	7	7	7	7	7	7	7	7
	Γ_T	5	14	7	12	0	4	4	0	7	0	0	5

a solution (x, y)*, to* (2.2)*, then* $x + q\sqrt{-d} = \gamma\beta^n$ *for some* $\beta \in \mathfrak{O}_D$ *and some* $\gamma \in \Gamma_{T(n)} := \cap_{l \in T(n)} \Gamma_l$*. In particular, if* $\Gamma_{T(n)}$ *is empty, then there is no solution for the equation* (2.2) *for the exponent* n*.*

Proof. Suppose that (x, y) is a solution to (2.2), then by Theorem 2.1 we have that there exists $\gamma \in \Gamma$ such that $x + q\sqrt{-d} = \gamma\beta^n$, where $\beta \in \mathfrak{O}_D$. Using the notation above it is easy to see that $\tau = \theta_1(x) = \theta_2(x) \in \mathcal{I}_l(D)$. Applying θ_i to both sides and taking the m-th powers (recall that $l = nm + 1$) we obtain

$$(\tau + q\theta_i(\sqrt{-d}))^m \equiv \theta_i(\gamma)^m \theta_i(\beta)^{l-1} \pmod{l}, \text{ with } \theta_i(\beta)^{l-1} \equiv 0 \text{ or } 1 \pmod{l}.$$

Thus $\gamma \in \Gamma_l$ as defined above, then the proposition follows. **QED**

So after calculating Γ we can calculate $\Gamma_{T(n)}$ for some set $T(n)$ of primes l satisfying conditions above. If $\Gamma_{T(n)}$ is empty there are no solutions, if not we may or may not, reduce the number of possible γ's to consider, that is the number of Thue equations that we must consider. To state the efficiency of this method, in terms of reducing the number of Thue Equations that we might have to consider at the beginning, just take a look at Table 2.1, when we consider the equation (**LN**). We can see for example that for $n = 3$ and $D = -53$ and -88 we are left with no Thue equations to consider after calculating Γ_T, for a suitable set of

primes T. The same happens for $D = -19, -66$ and -86 when $n = 5$ and for $D = -38, -62, -71$ and -77 when $n = 7$.

It is possible to see that when $D = 17$ or 33, after calculating Γ_T we reduce the number of equations almost in one-third.

Also, we can see that when n grows the number of D's for which there is a difference on the number of Thue equations to consider after Γ and Γ_T increases.

2.4 On eliminating and solving Thue equations

So far we have seen how to compute the Thue equations to get to the solutions of our Equation, the question that arises now is: are all of them needed? Do we only get the equations that come from a solution or do we get more than we need? The answer is: it depends on the equation.

Example 2.4.1. Let us consider $n = 5$, $D = -1$ and $C = 1$ in 2.2, so we have that $\mathfrak{O}_D = \mathbb{Z}$. After using Theorem 2.2, with $D = -1$ and the fact that our q is 1, we get the following Thue equations:

$$2 = \begin{cases} U^5 - V^5 \\ 2U^5 - 16V^5 \\ 16U^5 - 2V^5 \end{cases}, \quad 2x = \begin{cases} U^5 + V^5 \\ 2U^5 + 16V^5 \\ 16U^5 + 2V^5 \end{cases}$$

The two first equations give the solution $(x, y) = (0, -1)$, the two second one the solution $(x, y) = (1, 0)$ and the two last ones $(x, y) = (-1, 0)$. And these are all the solutions for (**LN**) when $D = -1$ and $n = 5$. So we have seen an example that all the Thue equations that we get come from a solution of our equation.

Consider now the same equation **LN** for $n = 5$ and let us put $D = -7$ in2.2. We have that $\mathfrak{O}_{-7} = \mathbb{Z}[\sqrt{7}]$, so we are in a real quadratic number field, with class number one. The Thue equations that we get after the using Theorem

2.1 are:

$$1 = \begin{cases} 3U^5 + 40U^4V + 210U^3V^2 + 560U^2V^3 + 735UV^4 + 392V^5 \\ 48U^5 + 635U^4V + 3360U^3V^2 + 8890U^2V^3 + 11760UV^4 + 6223V^5 \\ 765U^5 + 10120U^4V + 53550U^3V^2 + 141680U^2V^3 + \\ \qquad\qquad +187425UV^4 + 99176V^5 \\ 12192U^5 + 161285U^4V + 853440U^3V^2 + 2257990U^2V^3 + \\ \qquad\qquad 2987040UV^4 + 1580593V^5 \\ 49V^5 + 70U^3V^2 + 5UV^4; \end{cases}$$

$$x = \begin{cases} 8V^5 + 105U^4V + 560U^3V^2 + 1470U^2V^3 + 1960UV^4 + 1029V^5 \\ 127V^5 + 1680U^4V + 8890U^3V^2 + 23520U^2V^3 + 31115UV^4 + 16464V^5 \\ 2024U^5 + 26775U^4V + 141680U^3V^2 + 374850U^2V^3 + \\ \qquad\qquad +495880UV^4 + 262395V^5 \\ 32257U^5 + 426720U^4V + 2257990U^3V^2 + 5974080U^2V^3 + \\ \qquad\qquad +7902965UV^4 + 4181856V^5 \\ 245U^4V + 70U^2V^3 + V^5. \end{cases}$$

But we can see (using for that purpose a program like MAGMA) that none of the Thue equations of the first equality have solutions, therefore our equation, $x^2 - 7 = y^5$, has no solution. In this case all the Thue equations didn't come from any solution, for there are no solutions for (**LN**), when $D = -7$ and $n = 5$.

We will present three methods that will help us reduce further the number of Thue equations that we need to consider, in order to compute the solutions to the equation (2.2).

2.4.1 First elimination method: A relation between the coefficients

The first method is a very simple one. If we have

$$r = a_0U^p + a_1U^{p-1}V + \cdots + a_{p-1}UV^{p-1} + a_pV^p, \tag{2.20}$$

where r, U, V and all a_i's are integer numbers, then the $\gcd(a_0, a_1, \ldots, a_{p-1}, a_p)$ must divide r. So if this does not hold, we can discard the Thue equation. It is a simple method but can be extremely helpful.

2.4.2 Second elimination method: Local solvability

If a Thue equation has a solution then the same equation over an l-adic field, will also have a solution. Therefore, if we find an l-adic field over which the equation doesn't have a solution, then it won't have a solution at all over $\mathbb{Z}$. So we must test if each Thue equation is everywhere locally solvable. And to do that we will use Hensel's lemma (see Lemmas 2.1.1, 2.1.2 and 2.1.3).

These versions of Hensel's lemma allow us to work over a finite field, $\mathbb{F}_l$, with l a prime number, instead of working over an l-adic field, or even in the integers of the l-adic field. Of all these versions the one we are going to need is the third version, but even still we are going to restate it in a different way, to use it later.

Lemma 2.4.1 (Hensel's Lemma, version IV). *Let $f \in \mathbb{Z}[X_1, \ldots, X_m]$, a non-constant polynomial, l a prime number and let $\underline{a} = (a_1, \ldots, a_m) \in \mathbb{Z}^m$ have the property that, for some $k \geq 0$,*

$$f(\underline{a}) \equiv 0 \pmod{l^{2k+1}}$$

and, for some $i \in \{1, \ldots, m\}$,

$$\left(\frac{\partial f}{\partial X_i}\right)(\underline{a}) \not\equiv 0 \pmod{l^{k+1}}.$$

Then there exists an element $\underline{b} \in \mathbb{Z}_l^m$ *such that*

$$\begin{cases} \underline{b} \equiv \underline{a} \pmod{l^{k+1}} \\ f(\underline{b}) = 0 \end{cases}.$$

Proof. See [Mil06], Lemma 2.10 and Theorem 2.12. **QED**

Now consider

$$F(X, Y) = a_0 Y^n + a_1 X^{n-1} Y + \cdots + a_{n-1} X Y^{n-1} + a_n Y^n \in \mathbb{Z}[X, Y],$$

we want to solve the equation

$$F(X, Y) = c,$$

where c is an integer different from zero. Let l be a prime.

Lemma 2.4.2. *Let* $F(X, Y), c$ *and* l *as above. Let* x_1, y_1 *be integers such that:*

$$F(x_1, y_1) \equiv c \pmod{l}.$$

Then there exists $x, y \in \mathbb{Z}_l$ *such that*

$$\begin{cases} x \equiv x_1 \pmod{l}, \\ y \equiv y_1 \pmod{l}, \\ F(x, y) = c. \end{cases}$$

except possibly when $\left(\frac{\partial F}{\partial X}\right)(x_1, y_1) \equiv \left(\frac{\partial F}{\partial Y}\right)(x_1, y_1) \equiv 0 \pmod{l}$.

Proof. Consider x_1 and y_1 as in the lemma. Since we must have $\left(\frac{\partial F}{\partial X}\right)(x_1, y_1) \not\equiv 0 \pmod{l}$ or $\left(\frac{\partial F}{\partial Y}\right)(x_1, y_1) \not\equiv 0 \pmod{l}$, suppose, without loss of generality, that we are in the first case. Consider then $G(X) = F(X, y_1) - c$ and the lemma follows from the previous lemma. **QED**

So we only need to see if there is a solution for the equation $F(X, Y) \equiv c \pmod{l}$ that is not a solution for the partial derivatives of F modulo l.

Proposition 2.4.1. *Let $F(X, Y), c, l, x_1$ and y_1 as in the above lemma. Let n be the degree of F. If l does not divide nc, there exists $x, y \in \mathbb{Z}_l$ such that*

$$\begin{cases} x \equiv x_1 \pmod{l} \\ y \equiv y_1 \pmod{l} \\ F(x, y) = c \end{cases}.$$

Proof. By the previous lemma we only need to show that we must have or $\left(\frac{\partial F}{\partial X}\right)(x_1, y_1) \not\equiv 0 \pmod{l}$ or $\left(\frac{\partial F}{\partial Y}\right)(x_1, y_1) \not\equiv 0 \pmod{l}$. Suppose $\left(\frac{\partial F}{\partial X}\right)(x_1, y_1) \equiv \left(\frac{\partial F}{\partial Y}\right)(x_1, y_1) \equiv 0 \pmod{l}$. By Euler's homogeneous function theorem we have that

$$X\frac{\partial F}{\partial X}(X, Y) + Y\frac{\partial F}{\partial Y}(X, Y) = nF(X, Y).$$

Since $F(x_1, y_1) \equiv c \pmod{l}$, we have that

$$\begin{aligned} 0 &\equiv x_1\frac{\partial F}{\partial X}(x_1, y_1) + y_1\frac{\partial F}{\partial Y}(x_1, y_1) \pmod{l} \\ &\equiv nF(x_1, y_1) \pmod{l} \\ &\equiv nc \pmod{l}. \end{aligned}$$

Therefore l divides nc, but we have supposed the opposite. **QED**

Now, we only have to consider the case when l divides nc. Let $v \in \mathbb{N}_0$, such that $nc = l^v m$, and $\gcd(l, m) = 1$. We have the following, more general version, of the previous proposition

Proposition 2.4.2. *Let $F(X, Y), c, l$ as in the above lemma. Let n be the degree of F and v as above. Let x_1, y_1 be integers such that*

$$f(x_1, y_1) \equiv c \pmod{l^{2v+1}}$$

Then there exists $x, y \in \mathbb{Z}_l$ such that

$$x \equiv x_1 \pmod{l^{v+1}}, \quad y \equiv y_1 \pmod{l^{v+1}}, \quad F(x, y) = c$$

Proof. The case $v = 0$ was already done in the previous lemma. Now consider $v \geq 1$. So if we had both partial derivatives equal to zero modulo l^{v+1}, when substitute by a solution, (x_1, y_1), of $F(X, Y) \equiv c \pmod{l^{2v+1}}$ then, using once again the Euler's homogenous function theorem we have that:

$$\begin{aligned} 0 &\equiv x_1 \frac{\partial F}{\partial X}(x_1, y_1) + y_1 \frac{\partial F}{\partial Y}(x_1, y_1) \\ &\equiv nc \pmod{l^{v+1}}. \end{aligned}$$

Therefore l^{v+1} divides nc, which is impossible by our definition of v. So one of the partial derivatives is different from zero modulo l^{v+1}. Then the result follows from Hensel's lemma, version IV. **QED**

With this last result, we have found a way to test for each prime l the solubility of our Thue equation for the l-adic field $\mathbb{Q}_l$, without working with the l-adic field itself. Now, the only problem we seem to deal with is the fact that we cannot test this for each prime, since there are infinitely many primes. To overcome this problem we only need to use the Hasse-Weil Bound for the number of projective points on a curve defined over a finite field.

Theorem 2.5 (Hasse-Weil Bound). *Let C be a nonsingular projective curve defined on a finite field $\mathbb{F}_q$, with genus g. Denote by $N_C(q)$ the number of projective points on C that are defined over $\mathbb{F}_q$. Then we have*

$$|N_C(q) - (q+1)| \leq 2g\sqrt{q}.$$

Proof. See Corollary 2.5.27 on [Coh07b]. **QED**

So given $F(X,Y)$ a homogenous polynomial with integers coefficients of degree $n \geq 1$, and a non-zero integer c, our curve C will have as affine model $F(X,Y) = c$. The corresponding projective model is $F(X,Y) = cZ^n$, which has genus

$$g := \frac{(n-1)(n-2)}{2}.$$

Remember that we are looking for points on $C/\mathbb{F}_p$ such that Z is different from zero. When Z is equal to zero, we are talking about the points of C at infinity, and there are at most n points at infinity.

Lemma 2.4.3. *If $q \nmid nc\Delta_F$, where Δ_F is the discriminant of the polynomial F, and $q > 2g^2 + n - 1 + 2g\sqrt{g^2+n-1}$, then the equation $F(X,Y) = c$ has a solution over $\mathbb{F}_q$.*

Proof. Since $q > 2g^2 + n - 1 + 2g\sqrt{g^2+n-1}$, we have that $q + 1 - 2g\sqrt{q} > n$. And as we also have that $q \nmid nc\Delta_F$, we can apply the Hasse-Weil's Bound to see that our equation has a solution over $\mathbb{F}_q$ that is not a point at infinity. **QED**

So we only need to test the local solubility, using Proposition 2.4.2, for the primes $q \leq 2g^2 + n - 1 + 2g\sqrt{g^2+n-1}$ and for the primes $q \mid nc\Delta_F$.

2.4.3 Third elimination method: Finite solvability

So far we have been looking to the Thue equations of the type (2.6) or similar to this one. Now we will use some information of the Thue equations of the type (2.5). Let D, C and n be as before, (x, y) a solution of (2.2), then there are integers A and B such that

$$x = \frac{1}{2}\Big(\gamma(A + B\omega)^n + \overline{\gamma}(A + B\overline{\omega})^n\Big),$$

for a given pair $(\gamma, \overline{\gamma}) \in \Gamma$, where (A, B) is a solution of the Thue equation (2.6).

We have that $x = \frac{1}{2}\Big(\gamma(A + B\omega)^n + \overline{\gamma}(A + B\overline{\omega})^n\Big)$ is a Thue equation. So if we know that $l \mid x$, then we have that

$$\frac{1}{2}\Big(\gamma(A + B\omega)^n + \overline{\gamma}(A + B\overline{\omega})^n\Big) \equiv 0 \pmod{l}. \tag{2.21}$$

Furthermore if $v_l(x) = v > 0$, then

$$\frac{1}{2}\Big(\gamma(A + B\omega)^n + \overline{\gamma}(A + B\overline{\omega})^n\Big) \equiv 0 \pmod{l^v}. \tag{2.22}$$

So if we know that a prime $l \mid x$, with $v_l(x) = v$ and that for a given pair $\{\gamma, \overline{\gamma}\}$, the equation $\frac{1}{2}\Big(\gamma(A + B\omega)^n + \overline{\gamma}(A + B\overline{\omega})^n\Big) \equiv 0 \pmod{l^v}$ does not have solutions, then $\frac{1}{2}\Big(\gamma(A + B\omega)^n - \overline{\gamma}(A + B\overline{\omega})^n\Big) = 2q$ will not have a solution either.

This elimination method can be applied, when we have that $\gcd(D, C) > 1$, then for any $p \mid \gcd(D, C)$ we can test if the equation (2.21) has solutions or not. If $D = D_1 D_2$ and $C = D_1 D_3$, in first place we have that $D_1 \mid x$ and secondly, for all primes $l \mid D_1$, let $v = v_l(D_1)$ we can check if the equation (2.22) has solutions or not.

So if for a given prime l that we know that divides x the equation (2.21) or (2.22) has no solutions, we can eliminate the corresponding Thue equation (2.6).

The biggest problem with this method lays on the fact that in most cases we do not have any information on the primes that must divide x or not.

2.4.4 Computing solutions of a Thue equation

If after using the elimination methods we are still left with Thue equations, we have to see if they have solutions or not. For that, as it was said before, we need only to use the program `MAGMA`, for it has already a command to solve Thue equations. Even so we found useful to implement a method to help solve the equations, already referred in [BMS06]. The idea is to simplify the Thue equation (2.20) by minimizing its coefficients as much as possible. First of all we see if there is the need to make a change of coordinates so that the "leading coefficient" is the smallest possible, that is, changing U by V and vice-versa.

After this, we calculate $c = \gcd(a_0, a_1, \ldots, a_{n-1}, a_n)$ and divide each coefficient of and r by c (first elimination method). And thus we obtain a new Thue equation

$$\tilde{r} = b_0 U^n + b_1 U^{n-1} V + \cdots + b_{n-1} U V^{n-1} + b_n V^n,$$

where $\tilde{r} = r/c$ and $b_i = a_i/c$. and we have that now $\gcd(b_0, b_1, \ldots, b_{n-1}, b_n) = 1$.

The next step is to find a change of coordinates $U = \alpha\tilde{U} + \beta\tilde{V}$ and $V = \gamma\tilde{U} + \delta\tilde{V}$, with $\alpha, \beta, \gamma, \delta \in \mathbb{Z}$, such that, when we substitute these equalities in our Thue equation we get the following formula:

$$\tilde{r} = \tilde{U}^n + c_1 \tilde{U}^{n-1}\tilde{V} + \cdots + c_{n-1}\tilde{U}\tilde{V}^{n-1} + c_n \tilde{V}^n \tag{2.23}$$

and we must have $\alpha\delta - \beta\gamma = 1$ so that we have the map defined by

$$(\tilde{U}, \tilde{V}) \mapsto (\alpha\tilde{U} + \beta\tilde{V}, \gamma\tilde{U} + \delta\tilde{V})$$

is a bijection. This method is useful, due to the fact that when the coefficient a_m is very large, this greatly complicates the equation. In fact, in some of the equations that we get, the leading term has more than 10 digits, and this slows down the process of looking for a possible solution.

How to find α, β, γ and δ that satisfy the our requirements? If α and γ exists then they are a solution of the following Thue equation:

$$1 = b_0 U^n + b_1 U^{n-1} V + \cdots + b_{n-1} U V^{n-1} + b_n V^n,$$

So if our equation has a solution, then we just need to find β and δ, but as we must have $\alpha\delta - \beta\gamma = 1$, so α and γ are coprime so by the Euclid's Algorithm we can find β and δ. And finally, we make the change of coordinates and look for the solutions for the new Thue equation (2.23)

This work doesn't need to be done if our $\tilde{r}$ is equal to 1 (which happens quite often in the cases that we have considered) in this case we just need to ask for the solutions of the Thue equation and then try to compute a solution to (2.2).

And if a possible solution takes too much time to appear? For example when we considered the equation $x^2 - 43 = y^5$, one Thue equation that we have to solve is the following

$$\begin{aligned} &179337367525896U^5 + 5879968813306085U^4V + \\ &+77115068036135280U^3V^2 + 505677317944323310U^2V^3 + \\ &+1657973962776908520UV^4 + 2174412467160590233V^5 = 1. \end{aligned} \tag{2.24}$$

In the first attempts to solve this equation we end up waiting for more than two days for a solution, or no solution at all. In the end we got no answer at all, since the program seems to consume too much memory.

The same happens with following equation, for the equation $x^2 - 46 = y^5$.

$$-413653280369188080U^5 + 14027665230330336005U^4V \tag{2.25}$$
$$-1902805089698265168000U^3V^2 + 1290545201190390912460U^2V^3$$
$$-437645170630600988640UV^4 + 59365079254757981973 16V^5 = 1$$

In both cases, there is no need to apply the method described above, since our coefficient $\tilde{r}$ is already 1. So what to do to overcome this problem? Is it possible to find an substitution $\tilde{U}, \tilde{V}$ as before that could decrease the coefficients, or at least the coefficient of V^5? Let, as before,

$$r = b_0U^n + b_1U^{n-1}V + \dots b_{n-1}UV^{n-1} + b_nV^n$$

be our Thue equation. First we begin by considering $(\alpha, \gamma) \in \mathbb{Z}^2$ and define

$$b_{\alpha,\gamma} = \left|b_0\alpha^n + b_1\alpha^{n-1}\gamma + \dots b_{n-1}\alpha\gamma^{n-1} + b_n\gamma^n\right|. \tag{2.26}$$

Then given a, b positive integers define

$$B_{a,b} := \min\{b_{\alpha,\gamma} : (\alpha, \gamma) \in [-a, a] \times [-b, b]\}.$$

So we know that for a given pair $(a, b) \in \mathbb{N}^2$ there is an $(\alpha, \gamma) \in \mathbb{Z}^2$ such that $B_{a,b} = b_{\alpha,\gamma}$. It is easy to see that $\gcd(\alpha, \gamma) = 1$, otherwise there would be a prime $l \mid \gcd(\alpha, \gamma)$ and $b_{\frac{\alpha}{l},\frac{\gamma}{l}} = \frac{1}{l^n}b_{\alpha,\gamma}$. Then we find β and δ such that $\alpha\delta - \beta\gamma = 1$ and we apply the substitution $(\tilde{U}, \tilde{V}) = (\alpha\tilde{U} + \beta\tilde{V}, \gamma\tilde{U} + \delta\tilde{V})$ to our Thue equation (2.26) and we obtain a new equation

$$r = c_0\tilde{U}^n + c_1\tilde{U}^{n-1}\tilde{V} + \dots + c_{n-1}\tilde{U}\tilde{V}^{n-1} + c_n\tilde{V}^n,$$

where $c_0 = B_{a,b}$. So we find a solution $(\tilde{A}, \tilde{B})$ for this new Thue equation, remembering that a solution to the original Thue equation is given by $(A, B) = (\delta\tilde{A} - \beta\tilde{B}, -\gamma\tilde{A} + \alpha\tilde{B})$.

The best way for this process to work is to set $a, b \approx 10^3$ and apply this process as long as the new $B_{a,b} < \min\{b_0, b_1, \ldots, b_n\}$.

Let us see how it works with the Thue equations that we mentioned above. For both cases we will consider $a = b = 10^3$.

First we consider the Thue equation (2.24). After the first iteration we have the following Thue equation

$$133U^5 - 3005U^4V + 27160U^3V^2 - 122740U^2V^3 + 277340UV^4 - 250668V^5 = 1,$$

on the second iteration

$$4U^5 - 60U^4V - 180U^3V^2 - 360U^2V^3 - 345UV^4 - 133V^5 = 1$$

and this is how much we can minimize our Thue equation.

When we consider the Thue equation (2.25), after the first iteration we have the following Thue equation

$$U^5 + 15U^4V - 180U^3V^2 + 900U^2V^3 - 2220UV^4 + 2188V^5 = 1,$$

that is now as much minimal as we can get in terms of its coefficients, in absolute terms.

2.4.5 Final remarks

As we have said in the Introduction, most of the techniques can be already found on the literature, but not applied to the real quadratic extension case, due to the existence of a fundamental unit. Also most of the examples provided in this section deal with that particular case. The existence of a fundamental unit does not only imply a lot more Thue equations to work with but also some Thue equations with huge coefficients. We have seen some above, (2.24) and (2.25) for example.

This is caused by the "size" of the fundamental unit. For example, one of the fundamental units of $\mathfrak{O}_{-94}$ is $u = 2143295 + 221064\sqrt{94}$. Consider the equation $x^2 - 94 = y^5$. If we think that we have to calculate powers of the fundamental unit up to the fourth power, or instead a power where the exponent is between -2 and 2, it is fair enough to expected that the coefficients turn out to be extremely huge. If we didn't end up using the method to reduce the coefficients of a Thue equation, this last one for example and as the ones we have mentioned in 2.4.4, would not be solved by the existing routines in the programs already mentioned. In fact this method allows us to compute without much loss of time the solutions for the equation (2.1), with $p \in \{2, 3, 5, 7, 11\}$ for all our D in our range **R**. One may notice that all the examples given in this section have in common, first the equation (2.1), also the fact that $p = 5$, so it is possible to ask why not giving other examples with a different prime $p \geq 5$ or other equation. The reason for the choice of p first deals with the fact, that there are other methods more suitable for the case when $p \geq 7$, as we will see about it later on. Secondly, it possible to see that as p gets bigger, the time it takes to compute the Thue equations also increases. The use of the Thue equations method is recommended when considering specific cases of D and p, rather than for a huge amount of arbitrary values of D and/or of p, provided that p is bigger than 5.

It is possible also to use this method to calculate the solutions of equation (2.1) when $p = 2$ or 3, but it is much faster to use the procedure that we have stated on the section 2.2.2 for $p = 2$ or as we will see for $p = 3$ in section 2.5, than the method explained in this section.

In the Table 2.2 we give an account of how helpful or not the two methods (working alone or not) can be, considering again the equation (2.1) with $p = 5$.

Let us start with a comparison between the two methods. From what it is

possible to see in Table 2.2[1] (and in the rest of the results), the Local Solvability method helps us to eliminate more Thue equations than the Coefficient one; just take a look in the cases $D = 2, 6, 17, 68$ and 97, to confirm this observation. In fact, taking a look at what happens when we apply the method LST (local solubility test), having or not applied the method CT (coefficients test) before, we always end up with the same result. So we see that the method CT is not important at all. In fact the LST in a way uses CT, since in order for an equation to have solutions over a finite field it has to satisfy the CT. In terms of computation it runs much faster applying it before the LST.

Table 2.2: Efficiency of the elimination methods for the Thue equations

D	-2	-5	-6	-7	-17	-65	-68	-70	-79	-82	-97
$\#Cl_{\mathbb{K}_D}$	1	1	1	1	1	2	1	1	3	4	1
$\#\Gamma_T$[a]	4	4	5	5	10	8	15	4	5	4	4
$\#\Gamma_T$ + CT[b]	4	4	5	5	10	4	10	0	5	4	2
$\#\Gamma_T$ + CLST[c]	2	4	3	0	6	4	5	0	2	4	0
$\#\Gamma_T$ + LST[d]	2	4	3	0	6	4	5	0	2	4	0
Has solutions?	Yes	Yes	No	No	Yes	Yes	No	No	No	Yes	No
$\#\Gamma_T$ coming from a solution of C	2	2	0	0	4	2	0	0	0	2	0

[a] Number of Thue equations
[b] Coefficient elimination test
[c] Coefficient and local solubility elimination tests
[d] Local solubility elimination test

The LST seems to be the most efficient method to eliminate Thue equations, in cases like $D = -7, -70$ and -97 it eliminates every single equation, and in some cases that we have solutions, it leaves the only ones that matter, for example in the case $D = -2$, after the two methods being applied, we are left with two equations and it is possible to see that both come from the only solution

[1] The Thue equations all came from equations of the form $x^2 - D = y^5$

of that equation. But this is not the rule. In the case when $D = -68$ we are left with five equations but our equation (2.1) has no solution when $p = 5$. When considering $D = -6$ we are left with three equations and also none come from a solution. In the cases $D = -5, -10$ and -82 we are left with four equations and the solutions that exist only come from two, in each case. For $D = -17$ the solutions only come from four equations, when we are left with six equations. So though in some cases both methods (or only the LST) are very helpful, in some other cases they don't seem to help at all, since we don't eliminate or eliminate very few equations and the majority (sometimes all) of our Thue equations do not come from a solution.

2.5 Mordell's equation

In this chapter we will turn our attention to elliptic curves, mainly integral points over a special case of elliptic curves.

2.5.1 Integral Points over an elliptic curve

Putting $n = 3$ in (**LN**) and we get the following equation

$$x^2 = y^3 - D.$$

. The equation (2.27) is an elliptic curve, known as Mordell's equation, and we are interested in its integral points. Fortunately there are standard algorithms for computing the integral points on elliptic curves (see [Sma98, Chapter XIII], [GPZ98], [GPZ94]) Those methods are implemented in `MAGMA`. In order to keep the notation of the cited literature we ill use in this chapter the following notation

$$E_D : \quad x^2 = y^3 + D. \tag{2.27}$$

Before carrying on with the study of the Mordell's equation, we would like to mention the work of Hemer: he first solved Mordell's equation (2.27) for all $1 \leq |D| \leq 100$ (see [Hem54]).

We will give some more information about how to find some integral points, the torsion points, and give a description to know if there are any integral points or not.

Let us denote by $E_{D,\mathrm{tors}}(\mathbb{Q})$ the set of torsion points of the elliptic curve E_D defined over the rationals and $\mathcal{O}$ denote the point at infinity.

Proposition 2.5.1. *Let $P = (x, y)$ belong to $E_{D,tors}(\mathbb{Q}) \setminus \{\mathcal{O}\}$, then x, y are integers, that is P is a integral solution of E_D, and either $x = 0$ or $x \mid 3D$. Moreover, if $D = m^6 D_1$, where $v_p(D_1) < 6$, for any prime p, and m a nonzero integer, we have:*

(1) $E_{D,tors}(\mathbb{Q}) \simeq \mathbb{Z}/2\mathbb{Z}$ if and only if $D_1 \neq 1$ and is a cube;

(2) $E_{D,tors}(\mathbb{Q}) \simeq \mathbb{Z}/3\mathbb{Z}$ if and only if $D_1 = -432$ or $D_1 \neq 1$ and is a square;

(3) $E_{D,tors}(\mathbb{Q}) \simeq \mathbb{Z}/6\mathbb{Z}$ if and only if $D_1 = 1$;

(4) otherwise $E_{D,\mathrm{tors}}(\mathbb{Q})$ is trivial.

Proof. For the first part of the proposition, using the Nagell-Lutz Theorem (see [Coh07b, Theorem 8.1.10]) we have that P is an integral point, and that $x = 0$ or $x^2 \mid -27D^2 (= 3(3D)^2)$. Thus $X \mid 3D$. For the second part just see the proof of Proposition 8.1.13 of [Coh07b]. **QED**

So given D, it is possible to know all the torsion points and know how many we should expect.

Integral points of Mordell's equation

The search for integer and rational solutions (in fact more the non-existence of the solutions) for Mordell's Equation (2.27) has been studied for several years. Techniques using quadratic and cubic residues, unique factorization over number fields and/or binary cubic forms are well known. Therefore we will just state and try to sumarise some of the results known about the non-existence of integer solutions to Mordell's Equation(2.27).

Proposition 2.5.2. *Let a, b, m, n be integers, such that $D = ma^3 - nb^2$. The equation* (2.27) *has no integer solutions in the following cases:*

(i) $m = 1, n = 4, a \equiv 3 \pmod 4$ *and* $p \not\equiv 3 \pmod 4$, *whenever a prime* p *divides* b.

(ii) $m = n = 1, a \equiv 2 \pmod 4, b$ *is odd and* $p \not\equiv 3 \pmod 4$, *whenever we have a prime* p, *such that* $p \mid b$.

(iii) $m = n = 1, a \equiv 2 \pmod 4, b$ *is odd,* $3 \nmid b$ *and* D *is squarefree.*

(iv) $m = 2, n = 3, ab \neq 0, a \not\equiv 1 \pmod 3$, $3 \nmid b$, a *is odd if* b *is even and* $p = t^2 + 27u^2$ *is soluble in integers* t *and* u *if* p *is a prime such that* $p \mid a$ *and* $p \equiv 1 \pmod 3$. *Note that, if* $|a| < 7$, *there is no need for the last condition.*

(v) $m = 1, n = 4, a$ *is odd* $3 \nmid b$, $D \not\equiv 1 \pmod 8$ *and is also squarefree.*

(vi) $m = n = -1, a \equiv 2, 4 \pmod 8, b \equiv 1 \pmod 2$ *and* $p \not\equiv \pm 3 \pmod 8$ *if* $p \mid b$, *for a prime* p.

(vii) $m = -1, n = -2, a \equiv 4 \pmod 8$ *and* b *is not divisible by any prime* p *such that* $p \equiv 5, 7 \pmod 8$.

(viii) $m = n^3, n$ *is squarefree,* $n \equiv 1 \pmod 4, a \equiv -1 \pmod 4, b \equiv 0 \pmod 2$, $\gcd(n, b) = 1$ *and* $3 \nmid b$ *if* $n \equiv 1 \pmod 3$*; and lastly* a *and* b *have no common prime factor* p *such that the quadratic character* $(\frac{-n}{p}) = -1$.

(ix) $m = -1, n = -3, a \equiv 1 \pmod 4, b \equiv \pm 2 \pmod 6$ *and* b *has no prime factor* $p \equiv \pm 5 \pmod{12}$.

(x) $m = 8, a, b$ *are both odd,* $n = (-1)^t 2$*, where* $t = \frac{a-1}{2}$*,* $3 \nmid b$*, and if* $b \neq 1$ *then* D *is squarefree.*

Proof. For items (i)-(ix) you can consult the books [Coh07a, Proposition 6.7.6], [Mor69, Chapter 26], [Ros95, Section 14.4]. We will prove the item (x), the proof here presented is largely based on the proof of Proposition 6.7.6 in [Coh07a].

First some considerations about the possible integral solutions (x, y) of (2.27). We have $D = 8a^3 - nb^2$. If $n = 2$, then we have that $a \equiv 1 \pmod 4$. If either x or y is even, then both are, and we would have that $4 \mid x^2 - y^3 = D$, but $D \equiv 2 \pmod 4$, since b is odd. Then both x and y are odd and we must have $y \equiv 3 \pmod 4$, from the fact that the square of any odd number is congruent to 1 modulo 4, and that any cube of a odd number is congruent to itself modulo 4. In fact, in this case, we can go a little further and have the same equivalences if we replace modulo 4 by modulo 8. If $n = -2$, then we can check that $a \equiv 3 \pmod 4$. As before we also have that x and y are odd, but this time $y \equiv 7 \pmod 8$.

Suppose that (x, y) is an integral solution of $x^2 = y^3 + D$, so we would have also that (x, y) is an solution of

$$x^2 + nb^2 = y^3 + D + nb^2 = y^3 + 8a^3.$$

Note that $y^3 + 8a^3 = (y + 2a)(y^2 - 2ay + 4a^2)$. In each case we have that $x^2 + nb^2$

is an odd number, the same for $y \pm 2a$. Now we have that $y^2 - 2ay + 4a^2 = (y-a)^2 + 3a^2$. So $(y-a)^2 + 3a^2 \equiv 0 + 3 \equiv 3 \pmod 4$.

For $n = 2$, we then have that $x^2 + 2b^2 \equiv 3 \pmod 8$. By quadratic reciprocity we have that if p is a prime dividing $x^2 + 2b^2$, then $p \equiv 1, 3 \pmod 8$, for only in this cases we have -2 a quadratic residue modulo p. Suppose that $p \nmid b$, then since $a \equiv 1 \pmod 4$, we have that $2a \equiv 2 \pmod 8$, and also that $y + 2a \equiv 3 + 2 \equiv 5 \pmod 8$ and $(y-a)^2 + 3a^2 \equiv 4 + 3 \equiv 7 \pmod 8$. So therefore we have that there exists a prime $p \equiv 5, 7 \pmod 8$, that divides $x^2 + 2$, which contradicts what we have seen above. So p divides both b and x. If $b = 1$ we are done. Consider now the case that $b \neq 1$. We claim that $p \nmid (y + 2a)$. Indeed, since

$$(y-a)^2 + 3a^2 = (y + 2a)y + 4a^2,$$

if we had $p \mid (y + 2a)$ we would have $p \mid 4a^2$, so $p \mid a$, since $p = 2$ is impossible due to the fact that $p \mid x$, and x odd. But $p \mid a$ implies $p^2 \mid D = 8a^3 - 2b^2$, a contradiction since D is squarefree (assumption made for $b \neq 1$), thus proving our claim. Thus the p-adic valuation of $x^2 + 2b^2$ is equal to that of $(y-a)^2 + 3a^2$ hence is odd, a contradiction since this would again imply that $(\frac{-2}{p}) = 1$

For $n = -2$, an analogous reasoning proves our statement. In this case we have $x^2 - 2b^2 \equiv 1 - 2 \equiv 7 \pmod 8$. I p is a prime dividing $x^2 - 2b^2$, we have that $p \equiv 1, 7 \pmod 8$. Now we have that $a \equiv 3 \pmod 4$, so $2a \equiv 6 \pmod 8$. Hence we have that $y + 2a \equiv 7 + 6 \equiv 5 \pmod 8$ and $(y-a)^2 + 3a^2 \equiv 0 + 3 \equiv 3 \pmod 8$. So we must have a prime $p \equiv 3, 5 \pmod 8$ that divides $x^2 - 2b^2$. Therefore we must have $p \mid \gcd(b, y)$. If $b = 1$ then we are done, in the other case a similar reasoning from the case above help us to conclude the proof of the (x). **QED**

Example 2.5.1. Let us consider, once more, the case $D = 7$. We have that D and that $7 + 1 = 2^3$. So by the above proposition, item (iii) we have that $x^2 = y^3 + 7$ does not have any integral solutions. The same happens for $D = 6$, for we have $6 \equiv 2 \pmod 4$ and $6 + 2 = 2^3$, and $1 \not\equiv 3 \pmod 4$. Applying the above result we have, for $D = 6, 7, 215, 218, 998$ or 999 Mordell's equation E_D has no integral solutions. Proposition 2.5.2 shows there are no solutions to our equation for the following values of $D \leq 100$:

$$D = 6, 7, 11, 13, 23, 39, 47, 53, 61, 67, 83, 95.$$

Example 2.5.2. Consider now $D = 17$, it is possible to prove that the equation (2.27) in this case has 8 solutions, up to the sign of y, that are:

$$(x, y) = (4, 1), (3, 2), (5, 2), (9, 4), (23, 8), (282, 43), (375, 52), (378661, 5234).$$

For $n = 3$ or a multiple of 3, we end up using the facilities of our `MAGMA` implementation to find all the integral points in (**LN**) for the range (**R**)

Chapter 3

Frey curves and Modular Forms

The methods explained in Chapter 2 for solving (**LN**) are well known, and sometimes called the classical approach to solving a Diophantine equation. As we have said before, it works very nicely for small values of n, though as we have seen, sometimes we can get stuck on solving Thue equations even for a small value of n. From now on all the cases we are going to consider, we will have n a prime $p \geq 7$. Since we have D a negative integer, we will be considering the following equation

$$x^2 - D = y^p, \tag{3.1}$$

where in this case D is a positive integer in the range $1 \leq D \leq 100$.

3.1 Modular forms and the modular approach

Now we will introduce one of the most amazing tools for solving Diophantine equations, that consists of using a special elliptic curve, called a 'Frey curve' and the study of that curve using modular forms. This method has led to the resolution of many Diophantine problems, including the most notable of all Diophantine

equations, Fermat's Last Theorem, proved by Wiles ([Wil95]).

3.1.1 Newforms and Elliptic curves

The main object that we will be using are the *normalized newforms* of weight 2, without character on

$$\Gamma_0(N) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) : c \equiv 0 \pmod{N} \right\},$$

which we simply abbreviate to newforms of level N, a positive integer, where a newform is a modular form for a certain subgroup of $SL_2(\mathbb{Z})$ that is an eigenfunction of important operators called *Hecke operators*. Here are some facts about newforms (see [Coh07b, Chapter 15] for a brief summary of results or [DS05], [Miy06] or [Shi94] for more information):

- A newform f can be seen as a q-expansion

$$f = q + \sum_{n \geq 2} c_n(f) q^n \tag{3.2}$$

  with no term in q^0 and normalized so that the coefficient of q is equal to 1. The coefficients $c_n(f)$ will be called the *Fourier coefficients* of f.

- The field $\mathbb{K}_f = \mathbb{Q}(c_2(f), c_3(f), c_4(f), \dots)$ obtained by adjoining to $\mathbb{Q}$ the Fourier coefficients of f is a *finite and totally real* extension of $\mathbb{Q}$, in other words a totally real number field.

- The Fourier coefficients $c_n(f)$ are algebraic integers, in others words they belong to the ring of integers of $\mathbb{K}_f$.

- Let L be the Galois closure of $\mathbb{K}_f$. If f is a newform and σ is any element of $\mathcal{G}(L/\mathbb{Q})$, the Galois group of L with respect to $\mathbb{Q}$, then $f_\sigma =$

$q + \sum_{n\geq 2} \sigma(c_n(f))q^n$ is again a newform and called a conjugate of f. We will usually identify a newform with all of its conjugates.

- A newform satisfies the Ramanujan conjecture, proved by Deligne in the general case, that is, if l is a prime we have $|c_l(f)| \leq 2l^{1/2}$. Since this is also true for the conjugates of f, we have in fact $|\sigma(c_l(f))| \leq 2l^{1/2}$.

- For a given level N, the number of newforms (up to conjugacy or not) is finite. A formula can be found on [Coh07b] (see Proposition 15.1.1).

Using the formula mentioned in the last item, we can see that for the levels $N = 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 12, 13, 16, 18, 22, 25, 28$ and 60 there are no newforms.

A newform f is said to be *rational* when the field $\mathbb{K}_f$ is equal to $\mathbb{Q}$, that is, all the Fourier coefficients of f are rational integers. These newforms will be important for us. Now we state the modularity theorem for elliptic curves, proved by Wiles and successors (see [Wil95] , [TW95] and [BCDT01])

Theorem 3.1 (The Modularity Theorem for Elliptic Curves). *Let $N \geq 1$ be an integer. There is a one-to-one correspondence $f \mapsto E_f$ between rational newforms of level N and isogeny classes of Elliptic curves E defined over $\mathbb{Q}$ and of conductor equal to N. Under this correspondence, for all primes l not dividing N, we have $c_l(f) = a_l(E_f)$, where $c_l(f)$ is the l-th Fourier coefficient of f and $a_l(E_f) = l + 1 - |E_f(\mathbb{F}_l)|$, where $|E_f(\mathbb{F}_l)|$ is the number of $\mathbb{F}_l$-rational points on the elliptic curve E_f when considered over the finite field $\mathbb{F}_l$.*

The above theorem, which is one of the most notable achievements in number theory, is needed to go back and forth with ease between rational newforms

and elliptic curves. So far there is no need to understand in detail what is going on, we just have to keep in mind that each (isogeny class of) elliptic curve(s) of conductor N is associated to a rational newform of level N, and conversely. This is not at all what is going to happen with our second essential tool that we will be needing, which is Ribet's lowering theorem.

3.1.2 Ribet's level-lowering theorem

Given a newform f, an elliptic curve E and a prime l, we will denoted by c_l the lth Fourier coefficient of f and by $a_l(E) = l + 1 - |E(\mathbb{F}_l)|$.

Definition 3.1.1 (**arises from** see [Coh07b] Definition 15.2.1). *Let E be an elliptic curve over $\mathbb{Q}$ of conductor N, let f be a newform of level N', not necessarily equal to N, and let $\mathbb{K}_f$ be the number field generated by the Fourier coefficients of f. We will say that E arises modulo p from f, and write $E \sim_p f$, if there exists a prime ideal $\mathfrak{p}$ of $\mathbb{K}_f$ above p such that $c_l \equiv a_l(E) \pmod{\mathfrak{p}}$, for all but finitely many prime numbers l.*

Remark. Rather than saying that E arises modulo p from the newform f, it is usual here to say that the Galois representation

$$\rho_p^E : \mathcal{G}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathsf{Aut}(E[p])$$

arises from the newform f.

For instance, if $E = E_f$ is the elliptic curve of level N' corresponding to a rational newform f then $c_l = a_l(E)$ for $l \nmid N'$, so that $E \sim_p f$ for all primes p. On the other hand, if E is an elliptic curve of conductor N such that $E \sim_p f$ with f a rational newform of level N', then by the modularity theorem above we know that f corresponds to an elliptic curve $F = E_f$ defined over the rationals of conductor N', and we will also write $E \sim_p F$.

We can however be more precise than the definition (see [BS04]):

Proposition 3.1.1. *Assume that $E \sim_p f$. Then there exists a prime ideal $\mathfrak{p}$ of $\mathbb{K}_f$ above p such that ,for all prime numbers l, we have:*

(1) If $l \nmid pNN'$ then $a_l(E) \equiv c_l \pmod{\mathfrak{p}}$.

(2) If $l \| N$ but $l \nmid pN'$ then $c_l \equiv \pm(l+1) \pmod{\mathfrak{p}}$

However there is a slight but essential refinement of this proposition due to Kraus-Oesterlé [KO92], which is the final form of the definition of $\sim_p$ that we will use:

Proposition 3.1.2. *Assume that E and F are elliptic curves over the rationals, with respective conductors N and N', and assume $E \sim_p F$ as defined above. Then for all prime numbers l we have:*

(1) If $l \nmid NN'$ then $a_l(E) \equiv a_l(F) \pmod{\mathfrak{p}}$.

(2) If $l \| N$ but $l \nmid N'$ then $a_l(F) \equiv \pm(l+1) \pmod{\mathfrak{p}}$

The crucial refinement of this proposition is that we have removed the assumption that $l \neq p$. This will be important in terms of applications, since p will be an unknown exponent in the equations that we want to solve, and it would be very unpleasant to have conditions depending on p.

Let E be an elliptic curve defined over $\mathbb{Q}$. Let Δ be the discriminant for a minimal model of E, and N be the conductor of E, which can be obtained using an algorithm due to Tate (see Algorithms 5.1.3, 5.1.2 and 5.1.1). It is known N and Δ are related by the fact that $N \mid \Delta$ and that N and Δ have the same prime divisors, the primes of bad reduction.

Definition 3.1.2. *Keep the above notation and let p be a prime number. We define N_p by the formula*

$$N_p = N/ \prod_{\substack{q \| N \\ p | v_q(\Delta)}} q,$$

where $v_q(\Delta)$ is the q-valuation of Δ. So in other words, N_p is equal to N divided by the product of all prime numbers q such that $v_q(N) = 1$ and $p \mid v_q(\Delta)$.

It is important to have that the Δ in the definition of N_p is the discriminant of a minimal model of E.

Now we can state a simplified special case of Ribet's level-lowering theorem that will be sufficient for our applications (see [Rib90]).

Theorem 3.2 (Ribet's Level-Lowering Theorem). *Let E be an elliptic curve defined over the rationals and let $p \geq 5$ be a prime number. Assume that there does not exist a p-isogeny defined over $\mathbb{Q}$ from E to some other elliptic curve, and let N_p be as above. There exists a newform f of level N_p such that $E \sim_p f$.*

As mentioned, Ribet's theorem is more general than what we have stated, but the present statement is sufficient for our purposes. In Ribet's general theorem there is a modularity assumption, that we can discard in our statement due to the modularity theorem for elliptic curves.

In order to apply Ribet's level-lowering theorem, we have to overcome some technical difficulties. The most important one is the restriction that E should not have any p-isogenies defined over $\mathbb{Q}$, for simplicity we will say that E has no p-isogenies, in other words that there should be no subgroup of order p of E that is stable under conjugation (see [Coh07b], Definition 8.4.1). This unfortunately is not easy to check, but there are several results that help us in doing so. We give here two of the most useful.

Table 3.1: Pairs (l, j) corresponding to rational isogenies

l	j
11	$-2^{15}, -11^2, -11.131^3$
17	$-17.373^3/2^{17}, -17^2.101^3/2$
19	$-2^{15}.3^3$
37	$-7.11^3, -7.137^3.2083^3$
43	$-2^{18}.3^3.5^3$
67	$-2^{15}.3^3.5^3.11^3$
163	$-2^{18}.3^3.5^3.23^3.29^3$

Theorem 3.3. *Let $E/\mathbb{Q}$ be an elliptic curve with j-invariant j and let l be a prime. Then the Galois representation ρ_l^E is irreducible if (at least) one of the following conditions holds:*

(1) $l = 11$ or $l \geq 17$ and the pair (l, j) has no corresponding entry in Table 3.1,

(2) E has a rational 2-torsion point, $l \geq 7$ and

$$(l, j) \neq (7, -3^3.5^3), (7, 3^3.5^3.17^3),$$

(3) $l \geq 5$, E is semistable and all 2-torsion points are rational,

(4) $l \geq 11$ and E is semistable.

Proof. for a proof see [Dah08]. **QED**

Theorem 3.4 (**Diamond-Kramer** [DK95]). *Let E be an elliptic curve defined over $\mathbb{Q}$ of conductor N and let $p = 2, 3$. If $v_p(N) \geq 3$ and is odd, then ρ_l^E is irreducible for all primes $l \neq p$.*

Remark. If E has no p-isogenies then Ribet's theorem implies that $E \sim_p f$ for some newform f of level N_p. At that level there may be rational newforms, but also non-rational newforms defined over number fields of relatively large degree.

3.2 Frey curves

The general strategy for applying the tools that we have introduced so far in this section, to a Diophantine equation, is the following. We assume that our Diophantine equation has a solution, and to such solution we associate, if possible, an elliptic curve, called a Hellegouarch-Frey curve, or simply a Frey curve

3.2.1 The first Frey curve

One of the most interesting ideas in the proof of Fermat's last theorem, was the association of a given solution $a^p + b^p = c^p$, where p is an odd prime and a, b, c integers, to a particular elliptic curve given by the equation

$$Y^2 = X(X - a^p)(X + b^p), \qquad \textbf{(FLT)}$$

or equivalently,

$$Y^2 = X(X - a^p)(X - c^p).$$

This was first done by Yves Hellegouarch in his thesis [Hel72], but with a different purpose. Back then, Hellegouarch was trying to study the properties of the ramified division points over p. It was Gerhard Frey who first made a connection with the existence of a solution to the Fermat equations, which would originate an elliptic curve that could not exist, according to Serre's ϵ-conjecture and Taniyama-Shimura conjecture (see [Fre86]). This is why this curve is called nowadays *Frey curve*, though in some literature it is called *Frey-Hellegouarch* (see [Hel72] for the true origin of this curve). In 1990, Ribet proved the ϵ-conjecture, called nowadays Ribet's theorem ([Rib90]) and in 1995 Wiles, with the help of Taylor, finally proved the Taniyama-Shimura conjecture for a special case of elliptic curves, where the Frey curve could be included (see [Wil95] and [TW95]). Why does the Frey curve

works? The minimal discriminant for the Frey curve (**FLT**) is

$$\Delta_{min} = \frac{1}{2^8}(xyz)^p,$$

and the conductor is

$$N = 2\,\mathrm{Rad}(xyz).$$

Now looking back at Ribet's level lowering theorem, we have that if such curve existed the Galois representation associated to the curve would arise from a newform of level 2. But such newforms do not exist and Fermat's last theorem is proved.

3.2.2 Other examples of Frey curves

Nowadays one way to solve diophantine equations is using the modular approach, and therefore a Frey curve attached to the diophantine equation.

Consider for example a generalization of the Fermat equation

$$x^p + L^r y^p + z^p = 0$$

where x, y, z are non-zero integers, pairwise coprime, p is a prime greater than or equal to 5, L a prime number and $0 \leq r < p$. Let A, B, C be some permutation of $x^p, L^r y^p$ and z^p such that $A \equiv -1 \pmod 4$ and $2 \mid B$, and consider then the following Frey curve

$$E: \quad Y^2 = X(X - A)(X + B).$$

This example was studied by Serre, Kraus and Mazur. For the equation

$$x^2 = y^p + 2^m z^p$$

with x, y, z non-zero integers, with p prime and $m \geq 2$, we associate the following Frey curve

$$E: \quad Y^2 = X(X^2 + 2xX + y^p).$$

Following [Sikar] we present some recipe for ternary diophantine equations. By ternary Diophantine equations we mean equations of the form

$$Ax^l + By^m + Cz^n = 0 \tag{3.3}$$

the triple of exponents (l, m, n) is called the *exponent signature* of the equation (3.3). Which Frey curve is associated to a given exponent signature is detailed for three important exponent signatures $(p, p, p), (p, p, 2)$ and $(p, p, 3)$ respectively by Kraus [Kra97], by Bennett and Skinner [BS04] and by Bennett, Vatssal and Yazdani [BVY04].

Signature (p, p, p)

We start with the exponent signature (p, p, p). Suppose that A, B, C are non-zero pairwise coprime, $p \geq 5$ and $v_q(ABC) < p$, for every prime number q. Consider the equation $Ax^p + By^p + Cz^p = 0$, assuming that Ax, By, Cz are non-zero and pairwise coprime. Without loss of generality we also suppose that

$$Ax^p \equiv -1 \pmod 4, \quad By^p \equiv 0 \pmod 2.$$

The Frey curve associated is

$$E : Y^2 = X(X - Ax^p)(X + By^p).$$

The minimal discriminant is

$$\Delta_{min} \begin{cases} 2^4(ABC)^2(xyz)^{2p} & \text{if } 16 \nmid By^p, \\ 2^{-8}(ABC)^2(xyz)^{2p} & \text{if } 16 \mid By^p, \end{cases}$$

and the conductor N is given by

$$N = \begin{cases} 2\,\mathrm{Rad}_2(ABCxyz) & \text{if } v_2(ABC) = 0 \text{ or } v_2(ABC) \geq 5, \\ 2\,\mathrm{Rad}_2(ABCxyz) & \text{if } 1 \leq v_2(ABC) \leq 4 \text{ and } y \text{ is even}, \\ \mathrm{Rad}_2(ABCxyz) & \text{if } v_2(ABC) = 4 \text{ and } y \text{ is odd}, \\ 2^3\,\mathrm{Rad}_2(ABCxyz) & \text{if } v_2(ABC) = 2 \text{ or } 3 \text{ and } y \text{ is odd}, \\ 2^5\,\mathrm{Rad}_2(ABCxyz) & \text{if } v_2(ABC) = 1 \text{ and } 3 \text{ and } y \text{ is odd}. \end{cases}$$

And we have the following result due to Kraus.

Theorem 3.5 (Kraus [Kra97]). *Under the above assumptions, $E \sim_p f$ for some newform f of level N_p where*

$$N_p = \begin{cases} 2\,\mathrm{Rad}_2(ABC) & \textit{if } v_2(ABC) = 0 \textit{ or } v_2(ABC) \geq 5, \\ 2\,\mathrm{Rad}_2(ABC) & \textit{if } 1 \leq v_2(ABC) \leq 4 \textit{ and } y \textit{ is even}, \\ \mathrm{Rad}_2(ABC) & \textit{if } v_2(ABC) = 4 \textit{ and } y \textit{ is odd}, \\ 2^3\,\mathrm{Rad}_2(ABC) & \textit{if } v_2(ABC) = 2 \textit{ or } 3 \textit{ and } y \textit{ is odd}, \\ 2^5\,\mathrm{Rad}_2(ABC) & \textit{if } v_2(ABC) = 1 \textit{ and } 3 \textit{ and } y \textit{ is odd}. \end{cases}$$

Signature $(p, p, 2)$

For signature $(p, p, 2)$ we consider the equation

$$Ax^p + By^p = Cz^2, \quad p \geq 7 \text{ is prime},$$

where we assume that Ax, By, Cz are non-zero and pairwise coprime. We moreover suppose that, for all primes q we have

$$v_q(A) < p, \quad v_q(B) < p, \quad \text{and} \quad v_q(C) \leq 1.$$

Without loss of generality we may suppose that we are in one of the following situations:

(i) $ABCxy \equiv 1 \pmod 2$ and $y \equiv -BC \pmod 4$.

(ii) $xy \equiv 1 \pmod 2$ and either $v_2(B) = 1$ or $v_2(C) = 1$.

(iii) $xy \equiv 1 \pmod 2$, $v_2(B) = 2$ and $z \equiv -By/4 \pmod 4$.

(iv) $xy \equiv 1 \pmod 2, v_2(B) \in \{3, 4, 5\}$ and $z \equiv C \pmod 4$.

(v) $v_2(By^p) > 6$ and $z \equiv C \pmod 4$.

In cases (i) and (ii) we consider the curve

$$E_1 : \quad Y^2 = X^3 + 2CzX^2 + BCy^pX.$$

In cases (iii) and (iv) we consider

$$N_2^E : \quad Y^2 = X^3 + 2CzX^2 + \frac{BCy^p}{4}X,$$

and in case (v) we consider

$$E_3 : \quad Y^2 + XY = X^3 + \frac{Cz - 1}{4}X^2 + \frac{BCy^p}{64}X.$$

Theorem 3.6 (Bennett and Skinner [BS04]). *With assumptions and notation as above we have:*

(a) The minimal discriminant of E_i is given by

$$\Delta_i = 2^{\delta_i}C^3B^2A(xy^2)^p,$$

where $\delta_1 = 6, \delta_2 = 0$ and $\delta_3 = -12$.

(b) the conductor of the curve E_i is given by

$$N = 2^\alpha C^2 \operatorname{Rad}(ABxy),$$

where

$$\alpha = \begin{cases} 5 & \textit{if i=1, case (i)} \\ 6 & \textit{if i=1, case (ii)} \\ 1 & \textit{if i=2 , case (iii)}, v_2(B) = 2 \textit{ and } y \equiv -BC/4 \pmod 4 \\ 2 & \textit{if i=2 , case (iii)}, v_2(B) = 2 \textit{ and } y \equiv BC/4 \pmod 4 \\ 4 & \textit{if i=2 , case (iv) and } v_2(B) = 3 \\ 2 & \textit{if i=2, case (iv) and } v_2(B) = 4 \textit{ or } 5 \\ -1 & \textit{if i=3, case (v) and } v_2(By^7) = 6 \\ 0 & \textit{if i=3, case (v) and } v_2(By^7) \geq 7. \end{cases}$$

(c) suppose that E_i does not have complex multiplication (this would follow if we assume that $xy \neq \pm 1$). Then $E_i \sim_p f$ for some newform f of level

$$N_p = 2^\beta C^2 \operatorname{Rad}(AB)$$

where

$$\beta = \begin{cases} \alpha & \textit{case (i)-(iv)}, \\ 0 & \textit{case (v) and } v_2(B) \neq 0, 6, \\ 1 & \textit{case (v) and } v_2(B) = 0, \\ -1 & \textit{case (v) and } v_2(B) = 6. \end{cases}$$

Signature $(p, p, 3)$

Finally, for signature $(p, p, 3)$ we consider the equation

$$Ax^p + By^p = Cz^3, p \geq 5 \text{ is prime},$$

where we suppose, as before, that Ax, By, Cz are non-zero and pairwise coprime. We suppose without loss of generality that

$$v_q(A) < p, v_q(B) < p, v_q(C) < 3,$$

for all primes q, and that

$$Ax \not\equiv 0 \pmod 3, By^p \not\equiv 2 \pmod 3.$$

The Frey curve we consider is the following

$$E: \quad Y^2 + 3CzXY + C^2By^pY = X^3.$$

Theorem 3.7 (Bennett, Vatsal and Yazdani [BVY04]). *With notation and assumptions as above:*

(a) The conductor N of the curve E is given by

$$N = \mathrm{Rad}_3(ABxy)\,\mathrm{Rad}_3(C)^2\epsilon_3$$

where

$$\epsilon_3 = \begin{cases} 3^2 & \text{if } 9 \mid 2 + C^2By^p - 3Cz, \\ 3^3 & \text{if } 3 \mid\mid 2 + C^2By^p - 3Cz, \\ 3^4 & \text{if } v_3(By^p) = 1 \\ 3^3 & \text{if } v_3(By^p) = 2 \\ 1 & \text{if } v_3(By^p) = 3 \\ 3 & \text{if } v_3(By^p) > 3 \\ 3^5 & \text{if } 3 \mid C. \end{cases}$$

(b) Suppose that $xy \neq 1$ and the curve E does not correspond to one of the equations

$$1.2^5 + 27.(-1)^5 = 5.1^3, \quad 1.2^7 + 3.(-1)^7 = 1.5^3.$$

Then $E \sim_p f$ for some newform f of level

$$N_p = \mathrm{Rad}_3(AB)\,\mathrm{Rad}_3(C)^2\epsilon_3',$$

where

$$\epsilon_3' = \begin{cases} 3^2 & \textit{if } 9 \mid 2 + C^2By^p - 3Cz, \\ 3^3 & \textit{if } 3 \mid\mid 2 + C^2By^p - 3Cz, \\ 3^4 & \textit{if } v_3(By^p) = 1 \\ 3^3 & \textit{if } v_3(By^p) = 2 \\ 1 & \textit{if } v_3(By^p) = 3 \\ 3 & \textit{if } v_3(By^p) > 3 \textit{ and } v_3(B) \neq 3 \\ 3^5 & \textit{if } 3 \mid C. \end{cases}$$

3.2.3 How to choose a Frey curve

The key properties that a "Frey curve" E must have are the following:

- The coefficients of E depend on the solution of the Diophantine Equation.
- The minimal discriminant Δ of E can be written in the form $\Delta = C.R^p$, where R depends on the solution of the Diophantine equation, p is an unknown prime occurring as an exponent in the Diophantine equation, and most importantly C does not depend on the solution of the Diophantine equation, but only on the equation itself.
- If l is a prime dividing R then E has multiplicative reduction at l; in other words $v_l(N) = 1$, where N is the conductor of E.

The conductor N will be divisible by the primes dividing C and R, but because of the last condition above, the primes dividing R will be removed when computing N_p (see Definition 3.1.2); in other words, N_p is a divisor of N that is divisible only by primes dividing C, hence depending only on the equation. Without knowing the solutions to the Diophantine equation we can thus easily write a finite number of possibilities for N_p depending only on the equation. Using

Ribet's theorem we will then be able to list a finite set of newforms f such that $E \sim_p f$.

From then on we have to work more. Knowing the newform gives local information on the elliptic curve E, and since the equation of E has coefficients that depend on the solutions to the Diophantine equation, we may obtain useful information about these solutions, including of course the fact that they do not exist, as was the case for Fermat's Last Theorem.

The rest of this section will be devoted to applying these tools to obtain information about the solutions to our equation (3.1), even trying to solve it, when possible.

3.3 Multi-Frey approach

Now we begin the modular approach to the equation (3.1), but using as much information as we can from Frey curves, including several ones, instead of just one.

3.3.1 Removing common factors

As we will see later on, it is desirable when applying the modular approach to (3.1), for a prime $p \geq 7$, to remove the possible common factors of the three terms in the equation. This desire leads to a subdivision of cases according to the possible common factors, as seen in the following elementary lemma.

Lemma 3.3.1. *Suppose that* (x, y, p) *is a solution to* (3.1) *with* $p \geq 7$, $y \neq 0$ *and* D *in the range* $1 \leq D \leq 100$. *Then there are integers* d_1, d_2 *such that the following conditions are satisfied:*

(i) $d_1, d_2 \geq 1$;

(ii) $D = d_1^2 d_2$*;*

(iii) $\gcd(d_1, d_2) = 1$*;*

(iv) for all odd primes $q \mid d_1$ *we have* $(\frac{d_2}{q}) = 1$*;*

(v) if d_1 *is even then* $d_2 \equiv 1 \pmod 8$.

Moreover, there are integers s,t such that

$$x = d_1 t, \qquad y = \mathrm{Rad}(d_1)s,$$

$$t^2 - d_2 = es^p, \qquad \gcd(t, d_2) = 1, s \neq 0, \tag{3.4}$$

where

$$e = \prod_{\substack{q \mid d_1 \\ q \text{ prime}}} q^{p - 2v_q(d_1)} \text{ and } \mathrm{Rad}(e) = \mathrm{Rad}(d_1). \tag{3.5}$$

Proof. Let q be a prime that divides both x and D, which implies that q divides also y. Since D is in the range mentioned above, we have that $v_q(D) \leq 6$, in fact the equality only happens when we have $D = 64$ and $q = 2$, so in particular we have $v_q(D) < p$. Let $v = v_q(D)$, so we can write $x = q^r x_1$, $D = q^v D_1$ and $y = q^u y_1$ where $q \nmid x_1 D_1 y_1$. Now we rewrite our equation (3.1) in the following way:

$$q^{2r} x_1^2 - q^v D_1 = q^{up} y_1^p. \tag{3.6}$$

Now we have three possible cases $v < 2r$, $v > 2r$ and $v = 2r$. Let us consider the first case. So diving both sides of (3.6) by q^v we have the following equation: $q^{2r-v} x_1^2 - D_1 = q^{up-v} y_1^p$. Since $up \geq p > v$, we have $up - v > 0$ and $2r - v > 0$, so we conclude that $q \mid D_1$, which is impossible. We can reach the same conclusion when $2r < v$. So we can only have $v = 2r$, this means that $\gcd(x^2, D) = d_1^2$, where d_1 is an integer greater than zero. We can rewrite $x = d_1 t$ and $D = d_1^2 d_2$,

for some integers t, d_2, and by what we have seen above, we have also $\gcd(d_1, t) = \gcd(d_1, d_2) = 1$. Moreover, because

$$d_1^2 = \gcd(x^2, D) = \gcd(d_1^2 t^2, d_1^2 d_2) = d_1^2 \gcd(t^2, d_2),$$

we see that $\gcd(t^2, d_2) = 1$, equivalently, $\gcd(t, d_2) = 1$. Removing the common factors from $x^2 - D = y^p$ we obtain $t^2 - d_2 = es^p$, where e is given in (3.5) and $y = \mathrm{Rad}(d_1)s$. The integrality of e and the equality $\mathrm{Rad}(d_1) = \mathrm{Rad}(e)$ follow from the fact that $p \geq 7$ and from the facts mentioned above. We have thus proven (i), (ii) and (iii), it is easy to deduce (iv), about (v) we only need to see that $p - 2v_2(d_1) \geq 1$ and is always an odd number, so if $p - 2v_2(d_1) > 1$ and d_1 is even, then $8 \mid e$ and so $d_2 \equiv t^2 \equiv 1 \pmod 8$. We only need to consider the case that $p - 2v_2(d_1) = 1$, this means that $2v_2(d_1) = p - 1$, and since $2v_2(d_1) \leq 6$, we can only have $p = 7$ and $D = 64$, and so $d_1 = 8$. In this case our equation would be $t^2 - 1 = 2s^7$. So our $d_2 = 1 \pmod 8$, as desired. **QED**

Definition 3.3.1. *Suppose that D is a non-zero integer and (x, y, p) is a solution of* (3.1) *with $y \neq 0$ and p a prime greater than or equal to 7. Let d_1, d_2 be as in the above lemma and its proof. We call the pair (d_1, d_2) the signature of the solution (x, y, p). We call the triple (t, s, p) the simplification of (x, y) by the signature (d_1, d_2).*

With this terminology, Lemma 3.3.1 associates with any D a finite set of possible signatures (d_1, d_2) for the solutions (x, y, p) of (3.1) and $y \neq 0$. Then to solve (3.1) it is sufficient to solve it under the assumption that the solution's signature is (d_1, d_2) for each possible signature.

Example 3.3.1. For example if $D = 4$, there are two possible signatures satisfying the conditions of Lemma 3.3.1, these are $(d_1, d_2) = (1, 4)$ and $(2, 1)$. For the

second case we have then $x = 2t$ and $y = 2s$, and we must solve the equation

$$t^2 - 1 = 2^{p-2}s^p,$$

that has been solved by Siksek in [Sik03], where it is possible to see that we only have solutions when $p - 2 = 3$, but since $p \geq 7$, we know that this equation does not have any solution with $y \neq 0$. For the first signature we have that $x = t$ and $y = s$, and we have to solve the equation

$$t^2 - 4 = s^p, \qquad 2 \nmid st. \tag{3.7}$$

Since $t^2 - 4 = (t-2)(t+2)$ and $\gcd(t-2, t+2) = 1$, or we would have that $2 \mid s$, solving (3.7) would be the same as solving the following Thue equation: $4 = y_1^p - y_2^p$ using a recipe for the Diophantine equations of exponenet signature of the type $(p, p, 2), (p, p, 3)$ or (p, p, p). But so far we won't say anything about this equation until we apply the modular approach.

3.3.2 Two Frey curves

So now we intend to, given a solution to our equation (3.1), construct a Frey curve associated to it. But we will try to do a little bit more than that, we will construct not one, but two Frey curves associated to a given solution. We will try to demonstrate that, when possible, the use of several Frey curves is a more powerful tool for the study of Diophantine equations. This 'multi-Frey' approach often resolves with ease equations that would otherwise seem utterly hopeless.

We will use the method given by Ivorra-Kraus (see [IK06]) for Diophantine equations with signature $(p, p, 2)$, though in the section 3.2.2 we have considered the work of Bennett-Skinner (see [BS04]). While in the latter paper, we only get a Frey curve for each solution, in the former one we get two Frey curves for

each given solution to our equation, though they can be seen as twists of each other. Also in the latter paper the Frey curves that we obtain are minimal, while in the former, though the Frey curves we consider are not always minimal, we get conditions for the conductor N and for N_p for a given prime number p. Let p be a prime number great than or equal to 7, let a, b and c be nonzero rational integers, pairwise coprime. Consider the following equation

$$ax^p + by^p = cz^2. \tag{3.8}$$

Let (x, y, z) be a rational integer solution to (3.8), such that $\gcd(x, y, z) = 1$. We will define two elliptic curves E_1 and N_2^E over $\mathbb{Q}$, such that each one has at least one point of order 2 over $\mathbb{Q}$. To simplify our study of these two elliptic curves let us suppose that the following four conditions are satisfied:

E1: b is odd.

E2: c is square-free.

E3: If cz is odd, we can choose z in such way that we have $cz \equiv -1 \pmod 4$.

E4: The integers ax and by are coprime.

With this in mind we define our elliptic curves in the following way:

$$E_1 : \qquad Y^2 = X^3 + (2cz)X^2 + (acx^p)X; \tag{3.9}$$

$$N_2^E : \qquad Y^2 = X^3 + (2cz)X^2 + (bcy^p)X. \tag{3.10}$$

First we show that they are isogenous, up to a twist. Let us consider E_1. Consider $r = 4c^2z^2 - 4acx^p = 4cby^p$. We have that

$$F : \qquad Y^2 = X^3 - 4czX^2 + rX,$$

and E_1 are isogenous of degree 2 (see Example 4.5 in [Sil85]). Now replace X by $-2X$ in F and we have:

$$F^{(2)}: \qquad Y^2 = -8(X^3 + 2czX^2 + bcy^pX),$$

that is a quadratic twist of N_2^E.

Let us now apply this to our equation (3.1). Given D and one of its signatures (d_1, d_2) as in the Lemma 3.3.1, our equation can be seen in the following way:

$$d_2 1^p + es^p = 1.t^2$$

So since p is an odd prime greater than or equal to seven, we can make the following identifications

$$a = d_2, b = e, c = 1, x = 1, y = s \text{ and } z = t, \tag{3.11}$$

when d_1 is odd otherwise we make the following identifications:

$$a = e, b = d_2, c = 1, x = s, y = 1 \text{ and } z = t, \tag{3.12}$$

Given an integer D, a signature (d_1, d_2), we define for an integer t the following curves:

$$E(t): \qquad Y^2 = X^3 + (2t)X^2 + (d_2)X; \tag{3.13}$$

$$F(t): \qquad Y^2 = X^3 + (2t)X^2 + (t^2 - d_2)X. \tag{3.14}$$

Let D, (x, y, p), (d_1, d_2) and (t, s, p) be as in Lemma 3.3.1. From (3.11), (3.12), (3.9) and (3.10) we know that $E(t)$ (resp. $F(t)$) is E_1 (resp. N_2^E) when d_1 is odd and $E(t)$ (resp $F(t)$) is N_2^E (resp. E_1) when d_1 is even, through the above identifications. We can easily see that the discriminants of our curves $E(t)$ and

Table 3.2: Values for the conductors N_1 and N_2

Case	Conditions on d_1 and/or d_2	Conditions on s	N_2^E	N_2^F
(I)	$d_2 \equiv 4 \pmod{16}$	none	2^6	2^4
(I)	$d_2 \equiv 12 \pmod{16}$	none	2^6	2^2
(I)	$v_2(d_2) = 3$	none	2^6	2^5
(I)	$v_2(d_2) \in \{4, 5\}$	none	2^6	2^3
(I)	$v_2(d_2) = 6$	none	2^6	1
(I)	none	s even	2	2^6
(I)	$2v_2(d_1) = p - 3$	s odd	2^5	2^6
(I)	$2v_2(d_1) = p - 5$	s odd	2^3	2^6
(I)	$2v_2(d_1) \leq p - 7$	s odd	2	2^6
(II)	none	s even	2	2^6
(II)	$d_2 \equiv 1 \pmod{4}$	s odd	2^6	2^5
(II)	$d_2 \equiv -1 \pmod{4}$	s odd	2^5	2^6
(III)	none	none	2^7	2^7
(IV)	none	none	2^5	2^6

$F(t)$ will be one of the following quantities Δ_1, Δ_2 , according to the identifications made above

$$\Delta_1 = 2^6 e D^2 s^p, \qquad \Delta_2 = 2^6 e^2 D s^{2p}.$$

For the conductors we need to consider four cases:

(I) $D \equiv 0 \pmod{4}$.

(II) $D \equiv 1 \pmod{4}$.

(III) $D \equiv 2 \pmod{4}$.

(IV) $D \equiv 3 \pmod{4}$.

and then, using [IK06] is easy to see that we have that $N_{E(t)} = N_2^E \operatorname{Rad}_2(Ds)$ for the first curve, and for the second we have $N_{F(t)} = N_2^F \operatorname{Rad}_2(Ds)$, where N_2^E and N_2^F are given in Table 3.2.

Now let us take a look at the Galois representations of $\mathcal{G}(\overline{\mathbb{Q}}/\mathbb{Q})$ on the $E(t)[p]$ (resp $F(t)[p]$), the subgroup of p-torsion points of $E(t)(\overline{\mathbb{Q}})$ (resp. the subgroup of p-torsion points of $F(t)(\overline{\mathbb{Q}})$). We will denote this representation by $\rho_{1,p}$ in the case $E(t)[p]$ and by $\rho_{2,p}$ in the case $F(t)[p]$.

Proposition 3.3.1. *For $i \in \{1,2\}$ the representations $\rho_{i,p}$ are irreducible.*

Proof. Using Proposition 3.1 on [IK06] and the fact that $p \geq 7$, we have that the representations $\rho_{i,p}$ are irreducible, for $i \in \{1,2\}$. **QED**

So if we denote by $N_{E(t),p}$ (resp. $N_{F(t),p}$)) the 'conductor' defined in Definition 3.1.2, for the representation $\rho_{1,p}$ (resp. $\rho_{2,p}$). While from [IK06], Propositions 3.3 and 3.4 we get the Serre conductor for the representations $\rho_{i,p}$, for $i \in \{1,2\}$, we can use this results to compute our conductors and we have that :

$$N_{E(t),p} = N_2^E \operatorname{Rad}_2(D) \text{ and } N_{F(t),p} = N_2^F \operatorname{Rad}_2(D), \tag{3.15}$$

where N_2^E and N_2^F are given in Table (3.2). So we have that the representation $\rho_{1,p}$ (resp. $\rho_{2,p}$) arises from a newform of level $N = N_{E(t),p}$ (resp. $N = N_{F(t),p}$).

Definition 3.3.2. *If (t,s,p) is a solution of* (3.4) *and if the representation $\rho_{i,p}$ arises from a cuspidal newform f_i, for $i \in \{1,2\}$, then we say that solution (t,s,p) arises from the pair of newforms $\mathfrak{f} = (f_1, f_2)$ via the Frey curves $E(t)$ and $F(t)$.*

Example 3.3.2. Let $D = 7$, the only signature that we can have is $(d_1, d_2) = (1,7)$, and so we are in case (IV), and we have $N_{E(t),p} = 2^5 7$ and $N_{F(t),p} = 2^6 7$. For both quantities there are newforms of those respective level. For $D = 4$, as we have seen before we have two signatures $(d_1, d_2) = (1,4)$ and $(2,1)$. For the first case we have that $N_{E(t),p} = 2^6 = 64$ and $N_{F(t),p} = 2^4 = 16$. By one of our early remarks we see that there are no newforms of level 16, so there is no solution for

(3.1), with x and y coprime, for $p \geq 7$. In fact if were looking for newforms at level 64, we would find only one newform, and when applying the Ribet's theorem conditions, we would not find any obstacle to the existence to the fact that our elliptic curve E_1 arises modulo p from that (unique) newform of level 64. This simple example shows how the use of two Frey curves is important to solve a Diophantine equation, through this method. So we have that $t^2 - 4 = s^p$ has no solutions, with $s \neq 0$, for if $s = 0$, then we would have $t = \pm 2$.

For the second signature we have that $N_{E(t),p} = 2$ if s is even or $p \geq 9$ or $N_{E(t),p} = 8$ if $p = 7$, but in both cases there are no newforms of those levels, so the equation $t^2 - 1 = 2^{p-2}s^p$ has no solutions, as we have stated before. Just for case of completeness we have that $N_{F(t),p} = 2^6$.

Congruences and eliminating exponents

Given D and one of its signatures (d_1, d_2), let (t, s, p) be a solution of (3.4). So we know that (t, s, p) arises from the pair of newforms $\mathfrak{f} = (f, g)$, where f is a newform of level $N_{E(t),p}$ and g a newform of level $N_{F(t),p}$. Using the notation made in the beginning of this section for the Fourier coefficients of a newform and for the numbers $a_l(E)$, for an elliptic curve E and a prime l of good reduction, we have the following result:

Theorem 3.8. *With the notation above, suppose that the solution (t, s, p) arises from the pair $\mathfrak{f} = (f, g)$, where f is a newform of level $N_{E(t),p}$ and g a newform of level $N_{F(t),p}$, each one defined over a number field $\mathbb{K}_f$ and $\mathbb{K}_g$, respectively. Then there are places $\mathfrak{P}_f$ of $\mathbb{K}_f$ and $\mathfrak{P}_g$ of $\mathbb{K}_g$, both above p such that for every prime $l \nmid 2D$ we have:*

$$a_l(E(t)) \equiv c_l(f) \pmod{\mathfrak{P}_f}, a_l(F(t)) \equiv c_l(g) \pmod{\mathfrak{P}_g}, \text{ if } t^2 - d_2 \not\equiv 0 \pmod{l},$$

$$l+1 \equiv \pm c_l(f) \pmod{\mathfrak{P}_f}, l+1 \equiv \pm c_l(g) \pmod{\mathfrak{P}_g}, \text{ if } t^2 - d_2 \equiv 0 \pmod{l}.$$

Note that $t^2 - d_2 \not\equiv 0 \pmod{l}$ *is equivalent to say that* $l \nmid s$.

Proof. The result is standard (see [Kra98, Ser87, BS04, BMS06]); the conditions $l \nmid 2D$ and $l \nmid s$ simply say that l is a good prime of good reduction for $E(t)$ and $F(t)$, whereas the conditions $l \nmid 2D$ and $l \mid s$ imply that l is a prime of multiplicative reduction. The result follows from Proposition 3.1.1 **QED**

If f and g are both rational newforms, by Proposition 3.1.2 we have the following version of the previous theorem:

Theorem 3.9. *With the notation above, suppose that the solution* (t, s, p) *arises from the pair* $\mathfrak{f} = (f, g)$ *of rational forms, where* f *corresponds to an elliptic curve* E *and* g *to an elliptic curve* F. *Then for all the primes* $l \nmid 2D$ *we have:*

$$a_l(E(t)) \equiv a_l(E) \pmod{p}, \quad a_l(F(t)) \equiv a_l(F) \pmod{p}, \quad \text{if } t^2 - d_2 \not\equiv 0 \pmod{l},$$

$$l+1 \equiv \pm a_l(E) \pmod{p}, \quad l+1 \equiv \pm a_l(F) \pmod{p}, \quad \text{if } t^2 - d_2 \equiv 0 \pmod{l}.$$

Now we will give a method that will allow us to start to eliminate exponents p for the equation (3.4). The previous two results say that if (t, s, p) is a solution of (3.4) , then it arises from a pair of newforms of certain levels and all of these can be determined. Let us say that these pairs of newforms are $\mathfrak{f}_1 = (f_1, g_1), \ldots, \mathfrak{f}_n = (f_n, g_n)$. Then to solve (3.4) it is sufficient to solve it, for each i, under the assumption that the solution arises from pairs of newforms $\mathfrak{f}_i$.

We will now give one method to attack (3.4), under the assumptions that the solution arises from a particular pair of newforms (more will be presented in the following sections). If successful, the first method will prove that (3.4) has no solutions except possibly for finitely many exponents p and these are determined

by this method. This method is actually quite standard, as far it is known the basic idea is originally due to Serre [Ser87]. It is also found in Bennett and Skinner [BS04]. We shall present here a version that can be found in [BMS06].

Proposition 3.3.2 (Method I). *Let D, d_1, d_2 be a triple of integers satisfying Lemma 3.3.1 (i)-(v). Let $\mathfrak{f} = (f, g)$, be a pair of newforms, where f has coefficients in the ring of integers of the number field $\mathbb{K}_f$ and g has coefficients in the ring of integers of the number field $\mathbb{K}_g$. We denoted by $\mathcal{N}_f$ the norm map of $\mathbb{K}_f$ and by $\mathcal{N}_g$ the norm map of $\mathbb{K}_g$. If $l \nmid 2D$ is prime, let*

$$C_l(f, E) = \operatorname{lcm}\{\mathcal{N}_f(a_l(E(t)) - c_l(f)) : \ t \in \mathbb{F}_l, \ t^2 - d_2 \not\equiv 0 \pmod{l}\}$$

$$C_l(g, F) = \operatorname{lcm}\{\mathcal{N}_g(a_l(F(t)) - c_l(g)) : \ t \in \mathbb{F}_l, \ t^2 - d_2 \not\equiv 0 \pmod{l}\}$$

$$B_l'(f, E) = \begin{cases} C_l(f, E), & \text{if } (\frac{d_2}{l}) = -1, \\ \operatorname{lcm}\{C_l(f, E), \mathcal{N}_f((l+1)^2 - c_l(f)^2)\} & \text{if } (\frac{d_2}{l}) = 1, \end{cases}$$

$$B_l'(g, F) = \begin{cases} C_l(g, F), & \text{if } (\frac{d_2}{l}) = -1, \\ \operatorname{lcm}\{C_l(g, F), \mathcal{N}_g((l+1)^2 - c_l(g)^2)\} & \text{if } (\frac{d_2}{l}) = 1, \end{cases}$$

$$B_l(f, E) = \begin{cases} lB_l'(f, E), & \text{if } \mathbb{K}_f \neq \mathbb{Q}, \\ B_l'(f, E), & \text{if } \mathbb{K}_f = \mathbb{Q}, \end{cases}$$

$$B_l(g, F) = \begin{cases} lB_l'(g, F), & \text{if } \mathbb{K}_g \neq \mathbb{Q}, \\ B_l'(g, F), & \text{if } \mathbb{K}_g = \mathbb{Q}, \end{cases}$$

and

$$B_l(\mathfrak{f}) = \gcd\{B_l(f, E), B_l(g, F)\}.$$

If p is greater than 7, and if (t, s, p) is a solution to (3.4) *arising from the pair of newforms $\mathfrak{f} = (f, g)$, then p must divide $B_l(\mathfrak{f})$.*

Proof. The proposition follows almost immediately from Theorems 3.8 and 3.9. **QED**

Under the assumptions made (in this proposition), Method I eliminates all but finitely many exponents p, provided of course that $B_l(\mathfrak{f})$ is non-zero. Accordingly, we shall say that Method I is successful if there exists some prime $l \nmid 2D$ so that $B_l(\mathfrak{f}) \neq 0$. There are two situations where Method I is guaranteed to succeed.

- If one the newforms f, g is not rational, without loss of generality let us say that is f, then, for infinitely many primes l, the Fourier coefficients $c_l(f) \notin \mathbb{Q}$ and so all the differences $a_l(E(t)) - c_l(f)$, and $l + 1 \pm c_l(f)$ are certainly non-zero, immediately implying that $B_l(\mathfrak{f}) \neq 0$.

- Suppose that one of the newforms f or g is rational, let us say f, and so the corresponding elliptic curve E is defined over $\mathbb{Q}$. Suppose also that E has no non-trivial 2-torsion. By the Čebotarev Density Theorem we know that $\#E(\mathbb{F}_l)$ is odd for infinitely many primes l. Let $l \nmid 2D$ be any such prime. From the model for the Frey curve $E(t)$ we see that $E(t)$ has non-trivial 2-torsion, and so $l+1-a_l(E(t)) = \#E(t)(\mathbb{F}_l)$ is even for any value of $t \in \mathbb{F}_l, t^2 - d_2 \neq 0$. In this case $a_l(E(t)) - c_l(f) = a_l(E(t)) - a_l(E)$ must be odd and cannot be zero, similarly, the Hasse-Weil bound $|c_l| \leq 2\sqrt{l}$ implies that $l + 1 \pm c_l(f) \neq 0$. Thus $B_l(\mathfrak{f})$ is non-zero in this case and Method I is successful.

3.3.3 Kraus Method

The second method is adapted from the ideas of Kraus [Kra98] (see also [CS03] and [BMS06]). It can only be applied to one prime (exponent) p at a time and, if successful, it does show that there are no solutions to (3.4) for that particular exponent.

Let us briefly explain the idea of this second method. Suppose that f is a newform with Fourier expansion as in (3.2) and suppose that $p \geq 7$. Choose a small integer n so that $l = np + 1$ is prime with $l \nmid D$. Suppose that (t, s) is a solution of (3.4) arising from f. Working modulo l we see that $d_1^2 t^2 - D = y^p$ is either 0 or an $n - th$ root of unity. As n is small we can list all such t in $\mathbb{F}_l$ and compute $c_l(f)$ and $a_l(E(t))$ for each t in our list. We may then find that for no t in our list are the relations in Theorem 3.8 satisfied. In this case we have a contradiction and we deduce that there are no solutions to (3.4) arising from f for the exponent p.

Let us now write this formally. Suppose that $p \geq 7$ is a prime number and n an integer such that $l = np + 1$ is also prime and $l \nmid 2D$. Define

$$\mu_n(\mathbb{F}_l) = \{\zeta \in \mathbb{F}_l^* : \zeta^n = 1\} \text{ and } A(n, l) = \left\{\zeta \in \mu_n(\mathbb{F}_l) : \left(\frac{\zeta + D}{l}\right) = 0 \text{ or } 1\right\}.$$

For each $\zeta \in A(n, l)$, let δ_ζ be an integer satisfying

$$\delta_\zeta^2 \equiv (\zeta + D)/d_1^2 \pmod{l}.$$

It is convenient to write $a_l(1, \zeta)$ for $a_l(E_{\delta_\zeta})$. Notice that similar definitions are also applied to the newform g and Frey curve $F(t)$ and in this case we write $a_l(2, \zeta)$ for $a_l(F_{\delta_\zeta})$ We can now give our sufficient condition for the insolubility of (3.4) for the given exponent p.

Proposition 3.3.3 (Method II). *Let D, d_1, d_2 be a triple of integers satisfying Lemma 3.3.1 (i)-(v), and let $p \geq 7$. Let $\mathfrak{f} = (f, g)$ be a pair newforms defined over the number fields $\mathbb{K}_f$ and $\mathbb{K}_g$ respectively, that will be denoted $\mathbb{K}_1$ and $\mathbb{K}_2$ respectively. Let $c_l(1)$ (resp. $c_l(2)$) be the l-th coefficient of the Fourier expansion of f (resp. g). Let $\mathcal{N}_1$ (resp. $\mathcal{N}_2$) be the norm map of $\mathbb{K}_1$ (resp. $\mathbb{K}_2$). Suppose that there exist integers $n_1, n_2 \geq 2$ satisfying the following conditions.*

(a) The integers $l_1 = n_1 p + 1$ and $l_2 = n_2 p + 1$ are both prime and $l_1, l_2 \nmid D$.

(b) Either $\left(\frac{d_2}{l_i}\right) = -1$, or $p \nmid \mathcal{N}_i(4 - c_{l_i}^2(i))$, for $i \in \{1, 2\}$.

(c) For all $\zeta \in A(n_i, l_i)$, with $i \in \{1, 2\}$, we have

$$\begin{cases} p \nmid \mathcal{N}_i(a_{l_i}(i, \zeta) - c_{l_i}(i)), & \text{if } l_i \equiv 1 \pmod 4, \\ p \nmid \mathcal{N}_i(a_{l_i}(i, \zeta)^2 - c_{l_i}^2(i)), & \text{if } l_i \equiv 3 \pmod 4. \end{cases}$$

Then (3.4) *does not have any solutions for the given exponent p arising from the pair of newforms $\mathfrak{f}$.*

Proof. Suppose that the hypotheses of the proposition are satisfied and that (t, s) is a solution to (3.4).

Let $i \in \{1, 2\}$, first we show that $t^2 - d_2 \not\equiv 0 \pmod{l_i}$. Suppose otherwise. Thus $t^2 - d_2 \equiv 0 \pmod{l_i}$ and so $l_i \mid s$. In this case $(\frac{d_2}{l_i}) = 1$ and from part (b) we know that $p \nmid \mathcal{N}_i(4 - c_{l_i}^2(i))$. However, by Theorem 3.8 we know that $\pm c_{l_i} \equiv l_i + 1 \equiv 2 \pmod{\mathfrak{P}_i}$, where $\mathfrak{P}_i$ is a place of $\mathbb{K}_i$ above p and we obtain a contradiction showing that $t^2 - d_2 \not\equiv 0 \pmod{l_i}$.

From (3.4) and the definition of e in (3.5), we see the existence of some $\zeta \in A(n_i, l_i)$ such that

$$d_1^2 t^2 - D \equiv \zeta \pmod{l_i} \quad \textit{and} \quad t \equiv \pm \delta_\zeta \pmod{l_i}.$$

Replacing t by $-t$ in the Frey curves $E(t)$ and $F(t)$ has the effect of twisting the curve by -1 (this can be easily verified for each Frey curve on their definition (3.13) and (3.14)). Let $E_{1,t}$ be the Frey curve $E(t)$ and $E_{2,t}$ be the Frey curve $F(t)$. Thus $a_{l_i}(i,\zeta) = a_{l_i}(E_{i,t})$ if $l_i \equiv 1 \pmod 4$ and $a_{l_i}(i,\zeta) = \pm a_{l_i}(E_{i,t})$ if $l_i \equiv 3 \pmod 4$. Moreover by Theorem 3.8 $a_{l_i}(E_{i,t}) \equiv c_{l_i}(i) \pmod{\mathfrak{P}_i}$ for some place $\mathfrak{P}_i$ of $\mathbb{K}_i$ above p. This clearly contradicts (c). Hence, there is no solution to (3.4) arising from $\mathfrak{f}$ for the exponent p. **QED**

If one of the newforms in the pair $\mathfrak{f}$ is rational and moreover corresponds to an elliptic curve with 2-torsion, then it is possible to strengthen the conclusion of the previous Proposition by slightly strengthening the hypotheses. The following variant is far less costly in computational terms as we explain below.

Proposition 3.3.4 (Method II: 2-rational version). *Let D, d_1, d_2 be a triple of integers satisfying Lemma 3.3.1 (i)-(v), and let $p \geq 7$. Let $\mathfrak{f} = (f_1, f_2)$ be a pair newforms defined over the number fields $\mathbb{K}_{f_1}$ and $\mathbb{K}_{f_2}$ respectively, that will be denoted $\mathbb{K}_1$ and $\mathbb{K}_2$ respectively. Let $c_l(1)$ (resp. $c_l(2)$) be the l-th coefficient of the Fourier expansion of f_1 (resp. f_2). Let $\mathcal{N}_i$ be the norm map of $\mathbb{K}_i$, for $i = 1, 2$. Suppose that one of the f_i is a rational newform corresponding to elliptic curve $E/\mathbb{Q}$ with 2-torsion. Suppose that there exists an integer $n_i \geq 2$ satisfying the following conditions.*

(a) The integer $l_i = n_i p + 1$ is prime, $l_i < p^2/4$ and $l_i \nmid D$.

(b) Either $\left(\frac{d_2}{l_i}\right) = -1$, or $a_{l_i}(E)^2 \not\equiv 4 \pmod p$.

(c) For all $\zeta \in A(n_i, l_i)$ we have

$$\begin{cases} a_{l_i}(i,\zeta) \neq a_{l_i}(E), & \text{if } l_i \equiv 1 \pmod 4, \\ a_{l_i}(i,\zeta) \neq \pm a_{l_i}(E), & \text{if } l_i \equiv 3 \pmod 4. \end{cases}$$

Then (3.4) *does not have any solutions for the given exponent* p *arising from the pair of newforms* $\mathfrak{f}$.

Proof. Comparing this with Proposition 3.3.3 we see that is sufficient to show, under the additional assumptions, that if $a_{l_i}(i,\zeta)^2 \equiv a_{l_i}(E)^2 \pmod{p}$ then $a_{l_i}(i,\zeta) = \pm a_{l_i}(E)$, and if $a_{l_i}(i,\zeta) \equiv a_{l_i}(E) \pmod{p}$ then $a_{l_i}(i,\zeta) = a_{l_i}(E)$. Suppose that $a_{l_i}(i,\zeta)^2 \equiv a_{l_i}(E)^2 \pmod{p}$ (the other case is similar). Hence, $a_{l_i}(i,\zeta) = \pm a_{l_i}(E) \pmod{p}$. Now note that both elliptic curves under consideration here have 2-torsion. Hence, we can write $a_{l_i}(i,\zeta) = 2b_1$ and $a_{l_i}(E) = 2b_2$ for some integers b_1 and b_2. Moreover, by the Hasse-Weil bound we know that $|b_j| \leq \sqrt{l_i}$. Thus

$$b_1 \equiv \pm b_2 \pmod{p} \quad \textit{and} \quad |b_1 + b_2|, |b_1 - b_2| \leq 2\sqrt{l_i} < p$$

as $l_i < p^2/4$. Thus, $b_1 = \pm b_2$ and this completes the proof. **QED**

Let us now explain how this improves our computation. To apply Proposition 3.3.3 for some p we need to find a prime l satisfying conditions (a)-(c). The computationally expensive part is to compute $a_l(E_i) = c_l$ and $a_l(\zeta)$ for all $\zeta \in A(n,l)$. Let us, however, consider the application of Proposition 3.3.4 rather than Proposition 3.3.3. The computation proceeds as before by checking conditions (a), (b) first. When it comes to (c), we note that what we have to check the following

$$\begin{cases} \#E_{i,\zeta}(\mathbb{F}_l) \neq l + 1 - a_l(E_i), \text{ if } l \equiv 1 \pmod{4}, \\ \#E_{i,\zeta}(\mathbb{F}_l) \neq l + 1 \pm a_l(E_i), \text{ if } l \equiv 3 \pmod{4}, \end{cases}$$

for each $\zeta \in A(n,q)$. Rather than computing $a_l(\zeta)$ for each ζ, we first pick a random point in $E_{i,\zeta}(\mathbb{F}_l)$ and check whether it is annihilated by $l + 1 - a_l(E_i)$ if $p \equiv 1 \pmod{4}$ and either of the integers $l + 1 \pm a_l(E_i)$ if $p \equiv 3 \pmod{4}$. Only

if this is the case do we need to compute $a_l(\zeta)$ to test condition (c). In practice, for primes $p \geq 10^8$ this speeds up our computations for Method II.

Occasionally, Methods I and II fail to establish the non-existence of solutions to an equation of the form (3.4) for a particular exponent p even when it does seem that this equation has no solutions. The reasons for this failure are not clear to us. We, shall, however give a third method, rather similar in spirit to Kraus' Method (Method II, both versions), but requiring stronger global information furnished by Theorem 2.1 and more general than the method introduce in the section 2.3.2.

Suppose that D, d_1, d_2 are integers satisfying conditions (i)-(v) of Lemma 3.3.1. Let $E(t)$ and $F(t)$ be a pair of possible Frey curves associated with (3.4) and let $\mathfrak{f} = (f_1, f_2)$ be a pair of newforms, whose level is predicted in (3.15). Keeping the above notation, for $i \in \{1, 2\}$ define $T_l(f_i)$ to be the set of $\tau \in \mathbb{F}_l$ such that either:

- $p \mid \mathcal{N}_i(a_l(E_{i,\tau} - c_l(i)))$ and $\tau^2 - d_2 \not\equiv 0 \pmod{l}$; or
- $p \mid \mathcal{N}_i(l + 1 \pm c_l(i))$ and $\tau^2 - d_2 \equiv 0 \pmod{l}$.

We now suppose that D is not a square and follow the notation of section 2.2. We will now present a similar method use already in section 2.3.2 for the construction of Γ'. Fix a prime $p \geq 7$. Suppose that l is a prime satisfying the following conditions.

(a) $l \nmid 2D$.

(b) $l = np + 1$ for some integer n.

(c) $(\frac{d}{l}) = 1$, thus l splits in $\mathfrak{O}_D$, say $(l) = \mathfrak{l}_1\mathfrak{l}_2$.

(d) Each $\gamma \in \Gamma$ is integral at l; what we mean by this is that each γ belongs to the intersection of the localizations $\mathfrak{O}_{\mathfrak{l}_1} \cap \mathfrak{O}_{\mathfrak{l}_2}$.

We denote the two natural reduction maps by $\theta_1, \theta_2 : \mathfrak{O}_{\mathfrak{l}_1} \cap \mathfrak{O}_{\mathfrak{l}_2} \to \mathbb{F}_l$. These of course correspond to the two squareroots for d in $\mathbb{F}_l$ and are easy to compute.

Now, for $i \in \{1, 2\}$ let $\Gamma_l(f_i)$ be the set of $\gamma \in \Gamma$ for which there exists $\tau \in T_l(f_i)$ such that:

- $(d_1\tau - q\theta_1(\sqrt{d}))^n \equiv \theta_1(\gamma)^n$ or $0 \pmod{l}$; and
- $(d_1\tau - q\theta_2(\sqrt{d}))^n \equiv \theta_2(\gamma)^n$ or $0 \pmod{l}$.

Proposition 3.3.5 (Method III). *Let $p \geq 7$ be a prime. Let S be a set of primes l satisfying the conditions (a)-(d) above. With the notation as above, if the newform f_i belongs to a pair of newforms $\mathfrak{f}$, that gives rise to a solution (t, s) of* (3.4)*, then $d_1 t - q\sqrt{d} = \gamma\beta^p$ for some $\beta \in \mathfrak{O}_D$ and some $\gamma \in \Gamma_S(f_i) := \cap_{l \in S}\Gamma_l(f_i)$. In particular, if $\Gamma_S(f_i)$ or $\Gamma_S(f_1) \cap \Gamma_S(f_2)$ is empty, then the pair of newforms $\mathfrak{f}$ does not give rise to any solution to* (3.4) *for this exponent p.*

Proof. Suppose that (t, s) is a solution to (3.4) arising from the pair of newforms $\mathfrak{f} = (f_1, f_2)$ via the Frey curves $E(t)$ and $F(t)$, respectively. Fix i. Using the notation above, it is clear to see that $\theta_1(t) = \theta_2(t)$ is simply the reduction of t modulo l. Let $\tau = \theta_1(t) = \theta_2(t) \in \mathbb{F}_l$. It follows from Theorem 3.8 that $\tau \in T_l(f_i)$. Let (x, y) be the solution of (3.1) corresponding to (t, s). Thus $x = d_1 t$. We know by Theorem 2.1 that

$$d_1 t - q\sqrt{d} = \gamma\beta^p,$$

for some $\gamma \in \Gamma$ and $\beta \in \mathfrak{O}_D$. Applying θ_i to both sides and taking the n-th powers (recall that $l = np + 1$) we obtain

$$(d_1\tau - q\theta_i(\sqrt{d}))^n \equiv \theta_i(\gamma)^n\theta_i(\beta)^{l-1} \pmod{l} \quad \text{with } \theta_i(\beta)^{l-1} \equiv 0 \text{ or } 1 \pmod{l}.$$

Thus $\gamma \in \Gamma_l(f_i)$ as defined above. The proposition follows. **QED**

3.4 Some examples: Practical applications of the methods explained

We will now present some examples of applications of the methods studied so far, showing cases as only one method can work to show the non-existence of solutions to (3.1) for $p \geq 7$ or how they all work together for the same aim.

3.4.1 Non-existence of newforms

By Lemma 3.3.1, the exposition that follows and by Proposition 3.3.1 we can associate solutions of 3.1, having $p \geq 7$, with newforms of certain levels. If there are no newforms of the predicted levels, we immediately deduce that there are no solutions to (3.1). Using `MAGMA` to compute the newforms of the level associated to each equation (3.4), we found all D in our range ($\mathbf{R}$) where there are no newforms at the predicted levels. So we have the following result.

Proposition 3.4.1 (Absence of newforms). *Let D be an integer belonging to the list*

$$4, 12, 28, 32, 44, 60, 76, 92.$$

Then (3.1) *does not have any (non trivial) solutions for any prime $p \geq 7$. Moreover, if $D = 16$ and 64, with signatures $(d_1, d_2) = (1, 16)$ and $(1, 64)$ respectively, then the equation* (3.4) *does not have any (non trivial) solutions.*

Example 3.4.1. We have already seen that for $D = 4$, we failed on having newforms for some of the levels: with the signature $(d_1, d_2) = (1, 4)$ it failed for the levels predicted for the Frey curve $E(t)$. While for the signature $(d_1, d_2) = (2, 1)$, it was for the levels of the Frey curve $F(t)$.

Example 3.4.2. For $D = 12$, it is using the Frey curve $F(t)$ that we fail to have newforms for the predicted level, while for the Frey curve $E(t)$ for the predicted levels we had 4 newforms, two of them could be eliminated by level lowering, while with the other two we could not eliminate them with level lowering, and we couldn't eliminate any exponent $p \geq 7$ for either of them. For $D = 60$ it was also $F(t)$ which failed to have newforms for the predicted levels, and we would have a similar situation for the Frey curve $E(t)$ where some of the newforms could not be eliminated by level lowering and we would have all the exponents still to try. For $D = 92$ we also have the same situation for $F(t)$, while for $E(t)$, while most of the newforms eliminated by level lowering, we would still have two of newforms left, but each one could only give solutions for the exponent $p = 7$.

Example 3.4.3. For $D = 28, 32, 44, 76$, it was also the Frey curve $F(t)$ which failed to have newforms for the predicted levels, but in these cases, for the Frey curve $E(t)$ it was possible to eliminate all the newforms associated to the predicted level by the level lowering theorem.

Example 3.4.4. For $D = 16$ and 64 with signatures $(d_1, d_2) = (1, 16)$ and $(1, 64)$, respectively, we could see that for one of the Frey curves there was no newforms with the predicted level. But for the other signatures we can see that both Frey curves have associated newforms for the predicted levels, that cannot be eliminated by level lowering.

3.4.2 Non-existence of Solutions: Using Ribet's level lowering

We have seen the cases where there are no newforms. Now we will see cases, where we have newforms but we can eliminated them just using the level lowering theorem or a version of it that suits us better, Proposition 3.3.2. Still using the

program MAGMA for computation of newforms of certain levels and for implementing the method explained on the Proposition 3.3.2, we have the following result.

Proposition 3.4.2. *Let D be an integer belonging to the list*

$$6, 7, 11, 13, 14, 18, 19, 27, 34, 38, 40, 43, 46, 47, 54, 56, 58, 59, 79, 83, 86, 88, 91, 96$$

Then (3.1) *does not have any solutions for exponent a prime* $p \geq 7$.

Example 3.4.5. For $D = 7$ we only have the signature $(d_1, d_2) = (1, 7)$. Thus $t = x$ and $s = y$ and we need to solve the equation

$$t^2 - 7 = s^p, \quad \text{where } p \geq 7 \tag{3.16}$$

As $d_1 = 1$, by (3.11) we have associated to a solution (t, s, p) the following Frey curves:

$$E(t) : Y^2 = X^3 + 2tX^2 + 7X, \text{ and}$$
$$F(t) : Y^2 = X^3 + 2tX^2 + (t^2 - 7)X.$$

From Proposition 3.3.1 and Table 3.2 we know that any solution to (3.16) arises from a newform of level 224=$2^5 \times 7$ associated to the Frey curve $E(t)$ and from a newform of level $448 = 2^6 \times 7$ associated to the Frey curve $F(t)$.

Using MAGMA we find that there are, up to Galois conjugacy, precisely four newforms at level 224, these are

$$f_1 = q - 2q^3 - q^7 + q^9 - 4q^{11} + O(q^{12}),$$
$$f_2 = q + 2q^3 + q^7 + q^9 + 4q^{11} + O(q^{12}),$$
$$f_3 = q + \alpha q^3 + (\alpha + 2)q^5 + q^7 + (-2\alpha + 1)q^9 + (-2\alpha - 4)q^{11} + O(q^{12})$$
$$f_4 = q + \alpha q^3 + (-\beta + 2)q^5 - q^7 + (2\beta + 1)q^9 + (-2\beta + 4)q^{11} + O(q^{12}),$$

where α and β are such that:

$$\alpha^2 + 2\alpha - 4 = 0 \quad \text{and} \quad \beta^2 - 2\beta - 4 = 0.$$

For level 448, we find that there are, also up to Galois conjugacy, precisely ten newforms, that are

$$g_1 = q - 2q^5 - q^7 - 3q^9 + 4q^{11} + O(q^{12}),$$
$$g_2 = q + 2q^3 + q^7 + q^9 + O(q^{12}),$$
$$g_3 = q - 2q^3 + 4q^5 + q^7 + q^9 + O(q^{12}),$$
$$g_4 = q + 2q^3 - q^7 + q^9 + 4q^{11} + O(q^{12}),$$
$$g_5 = q + 2q^3 + 4q^5 - q^7 + q^9 + O(q^{12}),$$
$$g_6 = q - 2q^3 - q^7 + q^9 + O(q^{12}),$$
$$g_7 = q - 2q^5 + q^7 - 3q^9 - 4q^{11} + O(q^{12}),$$
$$g_8 = q - 2q^3 + q^7 + q^9 - 4q^{11} + O(q^{12}),$$
$$g_9 = q + \alpha q^3 + (-\alpha - 2)q^5 - q^7 + (-2\alpha + 1)q^9 + (-2\alpha - 4)q^{11} + O(q^{12}),$$
$$g_{10} = q + \beta q^3 + (\beta - 2)q^5 + q^7 + (2\beta + 1)q^9 + (-2\beta + 4)q^{11} + O(q^{12}),$$

where α and β are as before. The first two newforms (resp. first eight newforms) associated with $E(t)$ (resp. $F(t)$) are rational and so correspond to the two (resp. eight) isogeny classes of elliptic curves of conductor 224 (resp. 448). And it is possible to check that these elliptic curves have non-trivial 2-torsion, so by the remark made after Proposition 3.3.2 we might not be so successful in eliminating all but finitely many exponents p. But it turns out the opposite way,

$$B_3(f_1, E) = B_3(f_2, E) = 12 = 2^2 \times 3,$$
$$B_3(f_3, E) = B_3(f_4, E) = 240 = 2^4 \times 3 \times 5,$$

So we can see that no solutions to (3.16) arise from f_1 or f_2, because otherwise, we would have by Proposition 3.3.2 that $p \mid 12$, which contradicts $p \geq 7$, the same happens for f_3 and f_4, for if $p \mid 240$, then $p = 2, 3$ or 5, a contradiction. So only with the information of the newforms associated to the Frey curve $E(t)$ we conclude that (3.16) has no solutions for $p \geq 7$. For the sake of completeness we will also show what happens with the newforms associated to the Frey curve $F(t)$. In these cases we have

$$B_3(g_i, F) = 0, B_5(g_i, F) = 4 = 2^2, \text{ for } i \in \{1, 7\},$$
$$B_3(g_i, F) = 12 = 2^2 \times 3, \text{ for } i \in \{2, 3, 4, 5, 6, 8\},$$
$$B_3(g_9, F) = B_3(g_{10}, F) = 240 = 2^4 \times 3 \times 5.$$

So as before, we conclude that there are no solutions to (3.16) arise from the newforms associated to the Frey curve $F(t)$. Proving that (3.16) has no trivial solutions. So when $D = 7$, we have that the only solution to (**??**) is $(x, y, n) = (\pm 4, \pm 3, 2)$.

Example 3.4.6. As we have seen in the previous example, the level lowering helped us to eliminate all the newforms, associated to each of the Frey curves considered, and as is possible to see in the results obtained, this is what happens in the majority of the cases, where level lowering help us to show that there are no solutions for the equations considered. In the cases where $D = 43, 79, 83$ and 91 we have that the level lowering help us to eliminate all the newforms associated to one of the Frey curves, $E(t)$, while with the Frey curve $F(t)$ we still obtain some newforms to which we have finitely many powers left to exclude. When $D = 13, 91$ and 96 it is also possible to eliminate all the newforms associated to one of the Frey curves, $E(t)$ in the first case, $F(t)$ in the other cases, while for the other Frey curve, we find that there are some newforms we cannot exclude by level lowering and we still

have all the powers $p \geq 7$ left to exclude.

3.4.3 Non existence of solutions: Using Kraus' methods

So far we have seen the cases where with the non-existence of newforms or with the level lowering method, we could solve our equations, basically showing there were no solutions for a certain D, provided p is a prime greater than or equal to 7. Now let us turn to the cases where the methods of Kraus (Method II-Propositions 3.3.3 and 3.3.4, and Method III-Proposition 3.3.5) help us to solve our equation (3.1), when $p \geq 7$.

Proposition 3.4.3. *Let D be an integer belonging to the list*

$$23, 30, 39, 42, 51, 61, 62, 67, 70, 71, 74, 93.$$

Then (3.1) *does not have any (non trivial) solutions for $p \geq 7$ a prime number.*

We will now see examples where only Method II was the only required to show the none existence of solutions, others where Method III was the one who succeed in showing the non-existence of solutions and also examples where both methods where required.

Example 3.4.7. Let $D = 23$. The only possible signature is $(d_1, d_2) = (1, 23)$. Therefore we have $x = t$ and $y = s$. We are in case (IV), and there are 8 newforms of level $736 = 2^5 \times 23$ associated to the Frey curve

$$E(t) = Y^2 = X^3 + 2tX^2 + 23X,$$

and 26 newforms of level $1472 = 2^6 \times 23$ associated to the Frey curve

$$F(t) : Y^2 = X^3 + 2tX^2 + (t^2 - 23)X.$$

First we apply the level lowering (Method I) and we see that we are left with 2 newforms for each case, all of them predicting $p = 7$. The newforms are:

$$f_1 = q + \alpha q^3 + (-\alpha + 1)q^5 + (\alpha - 1)q^7 + (-2\alpha - 2)q^9 + (-3\alpha - 3)q^{11} + O(q^{12}),$$
$$f_2 = q + \beta q^3 + (\beta + 1)q^5 + (\beta + 1)q^7 + (2\beta - 2)q^9 + (-3\beta + 3)q^{11} + O(q^{12}),$$
$$g_1 = q + \beta q^3 + (-\beta - 1)q^5 + (-\beta - 1)q^7 + (2\beta - 2)q^9 + (-3\beta + 3)q^{11} + O(q^{12}),$$
$$g_2 = q + \alpha q^3 + (\alpha - 1)q^5 + (-\alpha + 1)q^7 + (-2\alpha - 2)q^9 + (-3\alpha - 3)q^{11} + O(q^{12}),$$

where $\alpha^2 + 2\alpha - 1 = 0$ and $\beta^2 - 2\beta - 1 = 0$.

We have that $B_3(f_i, E) = B_3(g_j, F) = 21 = 3 \times 7$ for $i, j \in \{1, 2\}$. Using Proposition 3.3.3, with $n = 16$, that is $l = 16 \times 7 + 1 = 113$ we have that no solution arises from a pair of newforms (f_i, g_j). So Method II was enough to solve this case. The same happens when $D = 61, 67$. For $D = 61$ the case is quite similar to this one, we are only left with the exponent $p = 7$ and all the newforms are irrational. For $D = 67$, using the level lowering, we are left with four newforms associated to the Frey curve $F(t)$, two of them predicting $p = 11$ and the other two $p = 17$. For the Frey curve $E(t)$ we are left with two newforms predicting $p = 17$. Therefore after Method I only predicts $p = 17$. After applying Method II, Proposition 3.3.3 since the newforms are irrational, we can discard this case.

Example 3.4.8. Let $D = 62$, then we have that there is only one possible signature $(d_1, d_2) = (1, 62)$, so $x = t$ and $y = s$. So we are in case (IV), and we have that there are 16 newforms of level $2^7 \times 31 = 3968$ associated to the Fey curve

$$E(t) : Y^2 = X^3 + 2tX^2 + 64X,$$

and 16 newforms of level 3968 associated to the Frey curve

$$F(t) : Y^2 = X^3 + 2tX^2 + (t^2 - 64)X.$$

After applying the level lowering we are left with 2 newforms in each case. Those newforms are

$$f_1 = q + \alpha q^3 + \frac{1}{2}(\alpha^5 + \alpha^4 - 8\alpha^3 - 6\alpha^2 + 12\alpha + 4)q^5 + \frac{1}{2}(-\alpha^4 + 6\alpha^2 - 4)q^7 + O(q^9),$$
$$f_2 = q + \beta q^3 + \frac{1}{2}(-\beta^5 + \beta^4 + 8\beta^3 - 6\beta^2 - 12\beta + 4)q^5 + \frac{1}{2}(\beta^4 - 6\beta^2 + 4)q^7 + O(q^9),$$
$$g_1 = q + \beta q^3 + \frac{1}{2}(\beta^5 - \beta^4 - 8\beta^3 + 6\beta^2 + 12\beta - 4)q^5 + \frac{1}{2}(-\beta^4 + 6\beta^2 - 4)q^7 + O(q^9),$$
$$g_2 = q + \alpha q^3 + \frac{1}{2}(-\alpha^5 - \alpha^4 + 8\alpha^3 + 6\alpha^2 - 12\alpha - 4)q^5 + \frac{1}{2}(\alpha^4 - 6\alpha^2 + 4)q^7 + O(q^9),$$

where α and β are such that:

$$\alpha^6 + 2\alpha^5 - 8\alpha^4 - 14\alpha^3 + 14\alpha^2 + 16\alpha - 4 = 0 \quad \text{and}$$
$$\beta^6 - 2\beta^5 - 8\beta^4 + 14\beta^3 + 14\beta^2 - 16\beta - 4 = 0.$$

Using Proposition 3.3.2, and denoting by $\mathfrak{f}_{i,j} = (f_i, g_j)$, for $i, j \in \{1, 2\}$ we have that

$$B_3(\mathfrak{f}_{i,j}) = 2^2 \times 3 \times 7,$$
$$B_5(\mathfrak{f}_{i,j}) = 2^3 \times 5 \times 7 \times 587,$$
$$B_7(\mathfrak{f}_{i,j}) = 2^3 \times 7^2 \times 13 \times 229,$$

for all $i, j \in \{1, 2\}$. So we conclude that there are no solutions arising from the pair $\mathfrak{f}_{i,j}$ with exponent $p > 7$. So let us see what happens with $p = 7$. Since each pair of newforms has both newforms irrational, we can only apply Proposition 3.3.3. Unfortunately we could not find any n and respective l that would satisfy the conditions of Proposition 3.3.3. We move to Method III, Proposition 3.3.5 And we see that with $S = \{29, 127\}$, we have that

$$\Gamma_S(\mathfrak{f}_{i,j}) = \emptyset$$

Therefore Method III alone managed to prove the non-existence of solutions for this case. We have a similar situation with $D = 30, 42$ and 74. For all of them after

applying Method I we were only left with the exponenet $p = 7$. When $D = 74$, we were also left with irrational newforms, while for the remaining cases all the newforms were rational.

Example 3.4.9. Let now $D = 39$. Also in this case we have only one signature possible, that is, $(d_1, d_2) = (1, 39)$, as also $t = x$ and $s = y$. So we are looking for solutions of the equation

$$t^2 - 39 = s^p, \quad p \geq 7. \tag{3.17}$$

Once again, we have the following Frey curves:

$$E(t) : Y^2 = X^3 + 2tX^2 + 39X,$$
$$F(t) : Y^2 = X^3 + 2tX^2 + (t^2 - 39)X.$$

So from $E(t)$ we might have solutions arising from newforms of level 1248 and from $F(t)$ we might have solutions arising from newforms of level 2496. After applying the level lowering method, we could not eliminate 2 newforms for the Frey curve $E(t)$ and 10 for the Frey curve $F(t)$. The two newforms of level 1248 left are:

$$f_1 = q + q^3 - 2q^5 + q^9 - 4q^{11} + O(q^{12}),$$
$$f_2 = q - q^3 - 2q^5 + q^9 + 4q^{11} + O(q^{12}).$$

It is possible to see that for $i \in \{1, 2\}$ we have

$$B_{53}(f_i, E(t)) = 2^4 \times 3^2 \times 5 \times 7 \times 11 \times 13,$$
$$B_l(f_i, E(t)) = 0, \quad \text{for } l \in \{5, 7, 11, 17, 19, 23, 29\}.$$

So we see that there are no solutions arising from f_1 and f_2 with exponent $p > 13$. If we consider one of the newform of level 2496, for example,

$$g = q - q^3 - 2q^5 + q^9 + O(q^{12}),$$

we would have $B_l(g, F(t)) = 0$, for all primes $l \in \{5, 7, 11, 17, 19, 23, 29, 31\}$. So in this case we would have all the possibilities for exponent still open. But taking into account the level lowering using the Frey curve $E(t)$ we know the only possibilities still left for p are 7, 11 and 13. Since both f_1 and f_2 are rational newforms, we have associated elliptic curves defined over $\mathbb{Q}$, let E_{f_1} be the elliptic curve defined by f_1 and E_{f_2} the elliptic curve defined by f_2. Then we have

$$E_{f_1} : Y^2 = X^3 + X^2 - 234X + 1296,$$
$$E_{f_2} : Y^2 = X^3 - X^2 - 234X - 1296.$$

that are respectively the elliptic curves 1248E1 and 1248H1 in Cremona's tables [Cre96]. It is also possible to see that they have a non trivial two torsion subgroup, so we can apply Proposition 3.3.4. For $p = 7$ or 13 we cannot find a value n that satisfies the assumptions of the Proposition just mentioned. But when $p = 11$, taking $n = 2$, that is, $l = 23$, we are able to verify all the assumptions of the Proposition 3.3.3, for both of the newforms f_1, f_2. So we have already eliminated $p = 11$. Then we are left to try Proposition 3.3.5. For $p = 7$ let $S = \{197, 281\}$, and for $p = 13$ let $S = \{131, 157, 313\}$. Then we have that, for $i \in \{1, 2\}$

$$\Gamma_S(f_i) = \emptyset,$$

showing that there are no solutions arising from any of the newforms f_1 and f_2 with exponent $p = 7$ or 13. We could have also have applied Method II and Method III to the newforms coming from the Frey curve $F(t)$ and reached the

same conclusions, provided that we would only test the primes $7, 11$ and 13, since we knew already there was no need to test all the others. If we had considered the newforms associated to the Frey curve $E(t)$ we would have almost the same scenario. For $p = 11$ and $p = 13$ the situation would be the same, that is, when predicted by a newform they would be eliminated by the same method as above, using the same primes l. For $p = 7$ the situation would be a bit different. There would be two irrational newforms that would be eliminated by using Method II, proposition 3.3.3, with the prime $l = 29$ verifying all the assumptions of the same proposition. For the rational newforms though most of them would behave as in the case of the Frey curve $F(t)$, just changing the set S, we would find two newforms that after applying Method III we would be left with a non-empty Γ_S for a certain S.

Therefore the equation (3.17) does not have any solutions for $p \geq 7$.

For $D = 30, 42, 51$ and 71 we have also the same situation. For $D = 51$, some of the newforms coming from one of the Frey curves that were not eliminated by the level lowering, leave all the options for exponent still open, while the newforms, coming from the other Frey curve, that also were not eliminated by level lowering, predict only a finite list of possible exponents. In all the other cases, in both Frey curves, we are only left with newforms that predict a finite list of possible exponents. So this also shows how the use of two Frey curves is more than welcome. For $D = 51, 70, 71, 93$ we have a similar situation, we need both methods to eliminate all newforms. When $D = 71$ after Method I, we are only left with the exponent $p = 7$. Though if we had only considered the Frey curve $F(t)$ alone we would have to consider $p = 17$ also. Method III alone helps to eliminate all the newforms associated with the Frey curve $E(t)$ for $p = 7$. But we need both methods II and III for the newforms associated to the Frey curve $F(t)$ when

$p = 7$. If we had considered $p = 17$, after method III we would have found a set S of primes such that Γ_S would be non-empty. For $D = 51$ we have to check the exponents $p = 7, 11$.

3.4.4 Possible solutions

We have seen so far the cases where we could prove the non-existence of solutions by non-existence of newforms, by applying the level lowering or by Kraus' methods. Now we shall see cases where all the previous methods failed in eliminating all the newforms associated to the Frey curves, that is, cases where Method III indicates that there might be a solution.

Proposition 3.4.4. *Let D be an integer belonging to the list*

$$31, 53, 66, 69, 78, 87, 95.$$

Then (3.1) *does not have any (non trivial) solutions for $p \geq 7$ a prime number.*

Example 3.4.10. Let $D = 78$, it is possible to see that there is only one signature for this case, that is $(d_1, d_2) = (1, 78)$, and so $t = x$ and $s = y$. We are looking for solutions of the equation

$$t^2 - 78 = s^p, \quad \text{for a prime } p \geq 7. \tag{3.18}$$

Our Frey curves are:

$$E(t) : Y^2 = X^3 + 2tX^2 + 78X,$$
$$F(t) : Y^2 = X^3 + 2tX^2 + (t^2 - 78)X,$$

which predict that we may have solutions to (3.18) arising from newforms of level 4992 in both cases. We see that there are 36 newforms at this level, up to Galois

conjugacy. After the applying the level lowering we are left with 6 newforms for each case and for each of them the only power left to test is $p = 7$. After applying Method II and Method III we are left with four newforms, two for each Frey curve, that are:

$$f_1 = q + q^3 + \frac{1}{4}(-\alpha^2 + 16)q^5 + 1\frac{1}{4}(\alpha^2 + 4\alpha - 16)q^7 + q^9 + 2q^{11} + O(q^{12}),$$
$$f_2 = q - q^3 + \beta q^5 + (\beta^2 + \beta - 4)q^7 + q^9 - 2q^{11} + O(q^{12}),$$

$$g_1 = q - q^3 + \frac{1}{4}(-\gamma^2 - 4\gamma + 16)q^5 + \frac{1}{4}(\gamma^2 + 8\gamma - 16)q^7 + q^9 - 2q^1 1 + O(q^{12})$$
$$g_2 = f = q + q^3 + \delta q^5 + (\delta^2 - \delta - 4)q^7 + q^9 + 2q^{11} + O(q^{12}),$$

where α, β, γ and δ are such that

$$\alpha^3 + 4\alpha^2 - 16\alpha - 48 = 0, \quad \beta^3 - 8\beta + 4 = 0,$$
$$\gamma^3 + 4\gamma^2 - 24\gamma + 16 = 0 \quad \text{and} \quad \delta^3 - 8\delta - 4 = 0.$$

For all of these newforms, Level lowering and Method II failed to eliminate them and for Method III, setting $\omega = \sqrt{78}$, we have that

$$\Gamma_{29}(f_i) = \Gamma_{29}(g_j) = \{5617 + 636\omega, 6688150613 + 757283934\omega\},$$

for $i, j \in \{1, 2\}$. Therefore we apply the method developed in 2.2 to solve our Thue equations for $p = 7$ associated to these two values, and we find that there are no solutions coming from those Thue equations. Therefore our equation (3.18) does not have any non trivial solution.

Example 3.4.11. For $D = 31, 53, 66, 78, 87$ and 95, we had only to look for solutions of Thue equations for $p = 7$, since the other possible powers were excluded after the several methods. For $D = 31, 53$ and 95, after level lowering, we had only the exponent $p = 7$ left for all the remaining newforms associated to the

Frey curve $E(t)$, while for the Frey curve $F(t)$. There were newforms with all exponents still possible; applying Proposition 3.3.2 we knew that if there was a solution arising from a newform, then we would have that $p = 7$.

For every case mentioned above, after applying Method II and III we were still left with the exponent $p = 7$. Therefore we proceeded to find the solutions for the mentioned D's when $p = 7$ using Thue equations and we found that there were no solutions.

Proposition 3.4.5. *For $D = 22$ and for $p \geq 7$ the equation* (3.1) *has the following solutions only*

$$(x, y, p) = \quad (\pm 47, 3, 7).$$

Also for $D = 94$ with $p \geq 7$, the equation (3.1) *has the following solutions only*

$$(x, y, p) = \quad (\pm 421, 3, 11).$$

Proof. For $D = 22$, we have the signature $(d_1, d_2) = (1, 22)$. So our equation (3.4) is essentially

$$t^2 - 22 = s^p,$$

for a prime $p \geq 7$. Our Frey curves are

$$E(t): \quad Y^2 = X^3 + 2tX^2 + 22X;$$
$$F(t): \quad Y^2 = X^3 + 2tX^2 + (t^2 - 22)X.$$

It is easy to see that the discrimant for the Frey curves are the following quantities

$$\Delta_{E(t)} = 2^6 22^2 s^p, \qquad \Delta_{F(t)} = 2^6 22 s^{2p}.$$

But on the other hand, the conductor associated to the represenations of both Frey curves is the same:

$$N_{E(t),p} = N_{F(t),p} = 2^7 \times 11 = 1408.$$

After applying level lowering we are left with the same 6 newforms for each Frey curve, all of them predicting the exponent $p = 7$. The newforms are:

$$f_1 = q - 2q^5 + 4q^7 - 3q^9 + q^{11} + O(q^{12}),$$
$$f_2 = q - 2q^5 - 4q^7 - 3q^9 - q^{11} + O(q^{12}),$$
$$g_1 = q + 2q^5 + 4q^7 - 3q^9 - q^{11} + O(q^{12}),$$
$$g_2 = q + 2q^5 - 4q^7 - 3q^9 + q^{11} + O(q^{12}),$$
$$f_3 = g_3 = q + \alpha q^3 + (-2\alpha + 1)q^5 + (-\alpha + 1)q^7 + (2\alpha - 2)q^9 - q^{11} + O(q^{12}),$$
$$f_4 = g_4 = q + \alpha q^3 + (2\alpha - 1)q^5 + (\alpha - 1)q^7 + (2\alpha - 2)q^9 - q^{11} + O(q^{12}),$$
$$f_5 = g_5 = q + \beta q^3 + (-2\beta - 1)q^5 + (\beta + 1)q^7 + (-2\beta - 2)q^9 + q^{11} + O(q^{12}),$$
$$f_6 = g_6 = q + \beta q^3 + (2\beta + 1)q^5 + (-\beta - 1)q^7 + (-2\beta - 2)q^9 + q^{11} + O(q^{12}),$$

where α is a solution of $X^2 - 2X - 1$ and β a solution of $X^2 + 2X - 1$, and the new forms $f_1, \ldots, f_6$ are associated to the Frey curve $E(t)$ and the newforms $g_1, \ldots, g_6$ to the Frey curve $F(t)$.

The newforms f_1, f_2, g_1 and g_2 are rational and the corresponding Elliptic curve has a non-trivial two-torsion subgroup. So we can use Method II, the rational version for these newforms, Proposition 3.3.4. After applying Method II to all the newforms in both cases, we eliminate f_3, f_6, g_4 and g_5 Now let $l = 29$ and $\mathfrak{f}_{i,j}$ be the pair of newforms (f_i, g_j) with $i \in \{1, 2, 4, 5\}$ and $j \in \{1, 2, 3, 6\}$ Using Method II we have that $\Gamma_{29}(\mathfrak{f}_{i,j})$ is

$$\{\emptyset\}, \qquad \text{if } 1 \leq i \leq 2 \text{ or } 1 \leq j \leq 2,$$
$$\left\{1, 42\omega + 197, (42\omega + 197)^2, (42\omega + 197)^5, (42\omega + 197)^6\right\} \quad \text{if } i \geq 3 \text{ or } j \geq 3,$$

where $\omega = \sqrt{22}$. Using now the Thue equations methods, we have that the only solution to (3.1) is the one mentioned in the proposition.

For $D = 94$ is more or the less as the same above, with the only exception that the exponent predicted is $p = 11$. **QED**

3.4.5 When and why does the Modular approach work?

After applying the Methods explained, there were some cases when we could not eliminate any exponent $p \geq 7$ for certain values of D. We will now explain why this might have happened.

The first case is when D is a square, that is,

$$1, 4, 9, 16, 25, 36, 49, 64, 81, 100.$$

For this case, using the notation above, $D = q^2$, so we have that the equation (3.1) has alays the following solution:

$$(x, y, p) = (\pm q, 0, p),$$

for any p prime greater or equal than 7. Notice that the solution is not a coprime one.

The second case is when D is a unit away from a square that is $D = q^2 \pm 1$. For the following values of D:

$$2, 3, 5, 8, 10, 15, 17, 24, 26, 35, 37, 48, 50, 63, 65, 80, 82, 99,$$

we will always have a coprime solution:

$$(|x|, |y|, p) = (q, 1, p),$$

where $q^2 = D \pm 1$ and p a prime greater and equal to 7.

For these two cases our equations have always a solution for any given prime.

Table 3.3: New equations for the values D in the third case

D	New equation	Solutions (x,y)
20	$x^2 - 4 = 5y^p$	$(\pm 3, 1)$
33	$x^2 - 33 = 8y^p$	$(\pm 5, -1)$
41	$x^2 - 41 = 8y^p$	$(\pm 7, 1)$
52	$x^2 + 4 = 13y^p$	$(\pm 3, 1)$
55	$x^2 - 11 = 5y^p$	$(\pm 4, 1)$
57	$x^2 - 19 = 3y^p$	$(\pm 4, -1)$
68	$x^2 - 17 = 16y^p$	$(\pm 1, -1)$
72	$x^2 - 9 = 8y^p$	$(\pm 1, -1)$
73	$x^2 - 73 = 8y^p$	$(\pm 9, -1)$
75	$x^2 - 15 = y^p$	$(\pm 4, 1)$
77	$x^2 + 7 = 11y^p$	$(\pm 2, 1)$
84	$x^2 - 4 = 21y^p$	$(\pm 5, , 1)$
85	$x^2 - 85 = 4y^p$	$(\pm 9, -1)$
90	$x^2 - 10 = 9y^p$	$(\pm 1, -1)$
97	$x^2 - 97 = 16y^p$	$(\pm 9, -1)$
98	$x^2 - 2 = 7y^p$	$(\pm 3, 1)$

The third case, as we will try to show in the next chapter, though it seems that there are no solutions for any prime p greater than or equal to 7, except for finitely many primes, we could not eliminate any of the exponents we were testing with the Methods explained in this chapter. But we can find a new equation with solutions for any given prime p. In Table 3.3, we present possible rearrangements of the equation (3.1) for the values D given also in Table 3.3.

It is possible to check that both Frey curves given by the work of Ivorra-Kraus [IK06] have the same levels if for a given value of D we consider the equation (3.1) or the one given in the Table 3.3. We see that, though the modular method is an effective method to solve Diophantine equations with no integral (rational) solutions, it does fail. The reason, is due to the fact that two different equations might originate Frey curves whose level predicted by Level lowering is the same,

and we can have one equation with solutions and the other with none.

In the next section, we will try to solve, when possible, the cases mentioned above.

Chapter 4

Bounding our variables x, y and p.

In this section we would like to present lower and upper bounds for x, y and p for the equation (3.1). For this purpose we will use some strategies that will use results on modular forms, on factorization over a number field and/or from linear forms in two and three logarithms. The cases that we could not solve so far and that have modular forms with infinitely many exponents left to eliminate are given in Tables 4.1, 4.3 and 4.4.

4.1 Bounds coming from modular forms

We start with a proposition similar to a result in [BMS06]

Proposition 4.1.1. *Suppose D is a non-zero integer and d_1, d_2 satisfy lemma 3.3.1. Suppose that (t, s, p) is a solution to* (3.4) *arising from a rational newform f via a Frey curve E_t or F_t. Then either $\mathrm{Rad}(s) \mid 2d_1$ or $|s| \geq (\sqrt{p} - 1)^2$.*

Proof. As the newform is rational, we know that the newform f corresponds to an

elliptic curve $E/\mathbb{Q}$ whose conductor equals the level of f. Suppose that $\mathrm{Rad}(s)$ does not divide $2d_1$. As t and d_2 are coprime we see that there is some prime $l \mid s$ so that $l \nmid 2D$. By Theorem 3.9 we see that p divides $l + 1 \pm a_l(E)$. It follows from the Hasse-Weil Bound (Theorem 2.5) that $l + 1 \pm a_l(E) \neq 0$, and so

$$p \leq l + 1 \pm a_l(E) < (\sqrt{l} + 1)^2,$$

again using Hasse-Weil. Thus $l > (\sqrt{p} - 1)^2$ and the proposition follows as we have that $l \mid s$. **QED**

4.1.1 Irrational newforms

The previous result only concerns rational forms, so first we have to see if after applying Level Lowering we are still left with irrational newforms. If this is the case we apply methods II and III for these irrational newforms to see if they arise from a solution or not. In case we are still left with some exponents, that will always be finitely many (see coments made after Proposition 3.3.2), we can apply the method of Thue equations to solve these cases.

Proposition 4.1.2. *Let D be one of the values in the Tables 4.1, 4.3 and 4.4, with signature (d_1, d_2) and suppose that (t, s, p) is a solution to* (3.4) *arising from a pair newforms $\mathfrak{f} = (f, g)$ via the Frey curve E_t and F_t, where one of the newforms, f or g is irrational. Then (D, t, s, p) is one of the following:*

$$(41, \pm 13, 2, 7), \quad (50, \pm 7, -1, 7) \quad (97, \pm 15, 2, 7).$$

Proof. First we begin to see which values of D have pairs of newforms $\mathfrak{f} = (f, g)$ in which one of them is irrational. We can easily see that for the following values

of D, there is no pair of newforms $\mathfrak{f}$ with at least one irrational newform,

$$1, 2, 3, 8, 9, 15, 16, 24, 36, 45, 48, 64, 72, 75, 81.$$

After applying Methods I, II and III, we were able to eliminate all the pairs of newforms $\mathfrak{f}$ containing an irrational newform for the following values of D.

$$5, 10, 15, 17, 20, 25, 26, 33, 35, 37, 52, 57, 63, 65, 68, 77, 80, 82, 84, 90, 98, 99, 100.$$

So the only possible pairs (D, p) left to consider are:

$$(29, 7), (41, 7), (50, 7), (73, 7), (85, 7), (97, 7), (98, 7).$$

After using the Thue equations, we get the solutions mentioned in the proposition.

QED

4.1.2 Some solutions from the rational newforms case

So now we can focus on rational forms f that might give rise to a solution to our equation (3.1). Let D be one of the values given in Tables 4.1,4.3 and 4.4. By Proposition 4.1.1 we have that, if (t, s, p) is a solution arising from f, then $\mathrm{Rad}(s)|2d_1$, where (d_1, d_2) is a signature of our equation (3.1) or $s \geq (\sqrt{p} - 1)^2$. Let us see what happens in the first case.

Proposition 4.1.3. *Let D be one of the values given in Table 4.4, and suppose that (x, y, p) is a solution of (3.1), with signature (d_1, d_2) and simplification (t, s, p), such that $\mathrm{Rad}(s)|2d_1$. Then (D, x, y, p) are the following:*

$$(41, \pm 13, 2, 7), (68, \pm 14, 2, 7), (68, \pm 46, 2, 11) \text{ or } (97, \pm 15, 2, 7).$$

For D in Table 4.3, with the same assumptions as before our solutions$(|x|, |y|, p)$ are $(q, 1, p)$, with p a prime great than or equal to 7 and q a natural number such that $|D - q^2| = 1$.

Proof. Suppose that D is one of the values in the tables mentioned and (x, y, p) is a solution to (3.1). By Lemma 3.3.1 we have that $x = td_1$ and $y = \mathrm{Rad}(d_1)s$, where (t, s, p) satisfy (3.4), for some d_1 and d_2 a signature of our equation (3.1) and we are assuming that $\mathrm{Rad}(s) \mid 2d_1$, so $\mathrm{Rad}(y) \mid 2d_1$.

When $\mathrm{Rad}(y) = 1$, then we are in the case that D is a unit away from a square, so D is one of the values of the table 4.3, and the solutions are $(|x|, |y|, p)$=$(q, 1, p)$, for all primes $p \geq 7$, and q such that $|D - q^2| = 1$.

Now suppose that $\mathrm{Rad}(y) = 2$ then [Beu81] shows that for the equation $x^2 + D = 2^m$, with $|D| < 2^{96}$ we must have $m \leq 18 + 2\log|D|/\log 2$. A short program implemented on MAGMA leads us to the solutions mentioned in the proposition. So now we only need to consider the following cases:

$$D = 90, \mathrm{Rad}(y) \in \{3, 6\} \text{ and } D = 98, \mathrm{Rad}(y) \in \{7, 14\}.$$

We have two cases, $\mathrm{Rad}(y) = l$ or $\mathrm{Rad}(y) = 2l$, with l an odd prime number. In the first case we are trying to find the solutions for the following equation

$$x^2 - D = l^m,$$

that is, equivalently, to solve the following equations:

$$x^2 - D = y^3,\ x^2 - D = ly^3 \text{ and } x^2 - D = l^2y^3.$$

So basically we are looking for integral points on elliptic curves where y is a power of l. Also after implementing a program on MAGMA we find that there aren't any solutions of the required form. In the case of $\mathrm{Rad}(y) = 6$, for $D = 90$, we would have $y = 2^a3^b$, therefore we had to solve the following equation $t_1^2 - 5 = 2^{ap-1}3^{ap-2}$, and since $a, b \geq 1$ and $p \geq 7$ we have that 5 is a square modulo 6,

which is absurd, so there is no solution in this case. For $D = 98$, if $y = 2^a 7^b$, since $ap, bp \geq 7$, $4 \mid y^p$ and $4 \mid x^2$ we would have that $4 \mid 98$, which is also absurd. **QED**

We have not dealt yet with the case of D being a square since it will be done in a rather different way in the next section.

So for the values D in Tables 4.3, 4.4 we have only to look for solutions (x, y, p) such that $y \geq (\sqrt{p} - 1)^2$.

4.2 Bounds for squares

Now we will take a look to the case when D is a square, so set $D = q^2$, with q a natural number. Our equation $x^2 - D = y^p$ can be written in the following way

$$(x - q)(x + q) = y^p.$$

Using unique factorization over the integers we have that

$$x - q = a y_1^p, \tag{4.1}$$

$$x + q = b y_2^p, \tag{4.2}$$

where $\gcd(a, b) = \gcd(x - q, x + q)$, and $\gcd(y_1, y_2) = 1$. Let us estimate $\gcd(x - q, x + q)$.

Proposition 4.2.1. *Let D be as above, (x, y, p) be a solution to* (3.1)*, with signature (d_1, d_2) and (t, s, p) the simplification of the previous solution by the*

Table 4.1: Case I: D is a square

D	$D \equiv \pmod 4$	(d_1, d_2)	c
1	1	$(1,1)$	1 or 2
9	1	$(1,9)$	1 or 2
		$(3,1)$	3 or 6
16	0	$(4,1)$	8
25	1	$(1,25)$	1 or 2
		$(5,1)$	5 or 10
36	0	$(1,36)$	1
		$(2,9)$	4
		$(3,4)$	3
		$(6,1)$	12
49	1	$(1,49)$	1 or 2
		$(7,1)$	7 or 14
64	0	$(8,1)$	16
81	1	$(1,81)$	1 or 2
		$(9,1)$	9 or 18
100	0	$(1,100)$	1
		$(2,25)$	4
		$(5,4)$	5
		$(10,1)$	20

signature just mentioned. Let $c = \gcd(x-q, x+q)$*, then we have that*

$$c = \begin{cases} 2d_1 & \textit{if } q \textit{ is odd and } x \textit{ is odd} \\ d_1 & \textit{if } q \textit{ is odd and } x \textit{ is even} \\ 2d_1 & \textit{if } q \textit{ is even and } d_2 \textit{ is odd} \\ d_1 & \textit{if } q \textit{ is even and } d_2 \textit{ is even} \end{cases}$$

Proof. Let $c = \gcd(x-q, x+q)$, so we have that $c \mid 2x$ and $c \mid 2q$, by the definition of the signature (d_1, d_2), we have that $d_1 \mid c$. On the other hand we have that $\gcd(x^2, D) = d_1^2$, it follows that $c^2 \mid 4d_1^2$ and so $c \mid 2d_1$.

Let us now distinguish the cases when q is odd or even. First suppose it is odd. We have that $x = d_1 t$, $D = d_1^2 d_2$ and $\gcd(t, d_2) = \gcd(d_1, d_2) = 1$. So if x

is even, then t is even also, and we have that y is odd, and since $c \mid y$ we have that c is odd, therefore $c = d_1$. If x is odd, then both numbers $x \pm q$ are even, therefore $2 \mid c$, so $c = 2d_1$.

Now we turn to the case where q is even. Suppose that d_2 is even. So we have that d_1 is odd, that is x and y are odd. So $c = d_1$.

If d_2 is odd, we see that this is equivalent to say that x is even, so we have again that both numbers $x \pm q$ are even, and that t is odd too. Let $d_3 = q/d_1$, that is still an integer. We have that d_3 is odd. So by definition we have that

$$\begin{aligned} c &= \gcd(x - q, x + q) \\ &= d_1 \gcd(t - d_3, t + d_3) \\ &= 2d_1 \gcd\Big(\frac{t - d_3}{2}, \frac{t + d_3}{2}\Big). \end{aligned}$$

And this ends the proof of our propostion. **QED**

For the values of D (a square) that we are still looking for possible solutions, the values of c are given in table 4.1.

First let us solve the case when $c = 1$, that is $x - q = y_1^p$ and $x + q = y_2^p$, where both y_1, y_2 are positive integers numbers, such that $\gcd(y_1, y_2) = 1$, and assume that $y_2 \geq y_1$. We have the following proposition:

Proposition 4.2.2. *Let $D = q^2$, $c = 1$ and (x, y, p) a solution to our equation* (3.1)*, and y_1 and y_2 as above. We have that*

$$p \leq 2q \text{ and } y_1^{p-1} \leq 2q.$$

Proof. So let y_1, y_2 be as above. By the equalities $x + q = y_2^p$ and $x - q = y_1^p$, we

have that

$$\begin{aligned} 2q &= y_2^p - y_1^p \\ &= (y_2 - y_1)(y_2^{p-1} + y_2^{p-2}y_1 + \cdots + y_2 y_1^{p-2} + y_1^{p-1}). \end{aligned}$$

Since y_2, y_1 are coprime, their difference is non-zero, that is, $(y_2 - y_1) \geq 1$. It is also easy to see that $y_2^{p-1} + y_2^{p-2}y_1 + \cdots + y_2 y_1^{p-2} + y_1^{p-1} \geq p y_1^{p-1}$. Now since $p y_1^{p-1} \geq \max\{p, y_1^{p-1}\}$, the proposition follows. **QED**

Therefore we implemented a simple program in `MAGMA` to compute y_1,y_2 and p and test if they give rise to a solution to our equation. After running the program we only found the following solution, $(x, y, p) = (\pm 12, 2, 7)$, when $D = 16$. This happens as we have not distinguished the cases when $c = 1$ or not in our program.

Suppose now that $c \neq 1$. Then by subtracting (4.1) and (4.2) we have that $2q = by_2^p - ay_1^p$, which it is possible to turn into an equation of the following form

$$By_2^p - Ay_1^p = C,$$

where $a = cA, b = cB, 2d = cC$ and $\gcd(A, B) = 1$. So we only need to solve these equations for each D and each value c associated to it. Though it seems a rather hard task, trying to solve other types of diophantine equations, fortunately the literature provides us with solutions for almost all the cases that we found and provides ways to find the solutions in the other cases (see section 3.2.2 for the recipes, and see [Ivo03], [BS04] and[BVY04] for solutions).

The equations we are going to find can be solved using the results concerning three types of diophantine equations, that can be sumarized in the following one

$$Au^p + Bv^p = Cw^k, \tag{4.3}$$

Table 4.2: Coeffiecients for our equations $E: \ Au^p + Bv^p = Cw^k$

D	c	AB	C	k
1	2	2^{p-2}	1	2
9	2	2^{p-2}	3	2
	3	3^{p-2}	2	3
	6	6^{p-2}	1	2
16	8	2^{p-6}	1	2
25	2	2^{p-2}	5	2
	5	5^{p-2}	2	2
	10	10^{p-2}	1	2
36	3	3^{p-2}	4	3
	4	2^{p-4}	3	2
	12	$2^{p-4}3^{p-2}$	1	2
49	2	2^{p-2}	7	2
	7	7^{p-2}	2	p
	14	14^{p-2}	1	p
64	16	2^{p-8}	1	2
81	2	2^{p-2}	9	2
	9	3^{p-4}	2	3
	18	$2^{p-2}3^{p-4}$	1	2
100	4	2^{p-4}	5	2
	5	5^{p-2}	4	2
	20	$2^{p-4}5^{p-2}$	1	2

with $p \geq k$. We say that equation (4.3) has signature (p, p, k). We notice that we only have three cases, all coming from three different exponent signatures $(p, p, 2)$, $(p, p, 3)$ and (p, p, p).

Before we prove our main goal, let us first find solutions to some equations of the signature (p, p, p) for a prime $p \geq 7$.

Proposition 4.2.3. *Let p be a prime greater than or equal to 7. Consider now the following equations:*

E_1: $7^{p-2}x^p + y^p - 2 = 0$;

E_2: $7^{p-2}x^p + 2^{p-2}y^p - 1 = 0$;

E_3: $14^{p-2}x^p + y^p - 1 = 0$.

None of the equations have solutions (x, y) *such that* $xyz \neq 0$.

Proof. Using the recipe given in section 3.2.2 for the equations of signature (p, p, p), we construct our Frey elliptic curves, estimate theirs conductors, as also the level for the newforms, and we apply the level lowering, Theorem 3.2, and we find out that there are no solutions to our equations arising from newforms of the predicted level, using for this a routine implemented on `MAGMA`, similar to the one used before. But for the sake of completeness we will show how to construct the Frey curves and what levels they correspond to. Consider the following equation

$$Au^p + Bv^p + Cw^p = 0,$$

where we assume $Au^p \equiv -1 \pmod 4$, $Bv^p \equiv 0 \pmod 2$. In the case E_1 we that $Bv^p = -2$ and $Au^p = \pm y^p$, since $7^{p-2}x^p \equiv y^p \pmod 4$. In the case E_2, we have $Bv^p = 2^{p-2}y^p$ and $Au^p = -1$, for the obvious reasons. For E_3 we have that $Bv^p = 14^{p-2}x^p$ and $Au^p = -1$. With these equalities we build our Frey curve, given by:

$$E: \ Y^2 = X(X - Au^p)(X + Bv^p).$$

In our cases we will have the following:

$$F_1(t): \ Y^2 = X(X \pm t)(X - 2);$$
$$F_2(s): \ Y^2 = X(X + 1)(X + \frac{1}{4}s);$$
$$F_3(u): \ Y^2 = X(X + 1)(X + 1 - u);$$

where $t = y^p$, $s = (2y)^p$ and $u = y^p$. We have that the expected levels $N_{p,i}$ for this curves are: $N_{p,2} = N_{p,3} = 14$ and $N_{p,1} = 2^5 \times 7$. By [Kra97], we have that $F_{i,v} \sim_p f$ for some newform f of level $N_{p,i}$, as given above, where $i \in \{1, 2, 3\}$ and $v \in \{t, s, u\}$. So as we said before, we use `MAGMA` to test the level lowering method and we see that there is no solution arising from a newform of the predicted level. **QED**

Now we are ready to prove the following result:

Proposition 4.2.4. *Let D be one of the values in table 4.1. Then the equation* (3.1)*, with p a prime number greater than or equal to 7 has no solutions with $y \neq 0$, except when $D = 16$, which the only solution is $(x, y, p) = (\pm 12, 2, 7)$.*

Proof. For each value of D and corresponding c, we apply the recipe (or the results found in the literature) for the signature (p, p, k) where k is given in the table 4.2. For $k = 2$, AB a power of 2 and $C = 1$ we use the Theorem 1 of [Ivo03], for the rest of the cases with $k = 2$ we use the results of [BS04]. For $k = 3$ we use the results on [BVY04], and for $k = p$ we use the Proposition 4.2.3, since the equations that we get are the eactly the ones that were stated in the Proposition just mentioned. After using those results we still are left with some cases: $p = 7$ for all the values of D in table 4.2 except $D = 1$ and 64, and $p = 11$ for $D = 64$ and 100. After using the Thue equations approach described in Proposition 2.2, the only solution we found was the one mentioned in the statement of the proposition. **QED**

So by now we have already found out all the solutions for equation (3.1), for all $p \geq 2$ with D a square.

4.3 A help from linear forms in logarithms

Now we proceed to find all the solutions for the values given in Table 4.4 and also give some bounds for the values in Table 4.3, since these last ones are by far the hardest case to solve that we have found so far. So let D be one of those values, let (x, y, p) be a solution, with $p \geq 7$ and $y \neq 0$. We have seen by now that this solution must arise from a rational newform f and that

$$y \geq (\sqrt{p} - 1)^2. \tag{4.4}$$

Kraus' methods, methods II and III presented in section 3.3.3, can help us find all possible cases where there might be a solution up to $p \leq 10^8$, possibly 10^9. So we can assume from now on that

$$p \geq 10^3, \tag{4.5}$$

and we will also have that

$$|x| \geq 10^3. \tag{4.6}$$

These inequalities are sufficient for much of our later work.

In the remainder of this section we always write $D = q^2 d$, where d is square free, and (x, y, p) will always be a solution to (3.1) satisfying the above inequalities, with signature (d_1, d_2) and simplification (t, s, p). We will also write down the linear form in logarithms corresponding to (3.1) and apply a theorem of Matveev to obtain upper bounds for the exponent p. These upper bounds will be far from the bounds that we have already imposed, but will help us to obtain other new bounds from more recent work on linear forms in logarithms.

We start our exposition with a definition that can be found in the literature (see for example [Coh07b, Chapter 12]).

Definition 4.3.1 (See Definition 12.1.1 in [Coh07b]). *Let $\mathbb{K}$ be a number field of degree n, let $\alpha \in \mathbb{K}^*$ be of degree $m \mid n$ and let*

$$P(X) = \sum_{k=0}^{m} a_k X^k = a \prod_{i=0}^{m} (X - \alpha_i)$$

be its minimal polynomial in $\mathbb{Z}[X]$, with $a_m \neq 0$, and the α_i's are the conjugates of α. We define the logarithmic height $\mathrm{h}(\alpha)$ by the following formula:

$$\begin{aligned} \mathrm{h}(\alpha) =& \frac{1}{m}\Big(\log(|a_m|) + \sum_{1 \leq i \leq m} \max(\log(|\alpha_i|), 0)\Big) \\ =& \frac{1}{n} \sum_{v \in \mathcal{P}(\mathbb{K})} \max\{\log |\alpha|_v, 0\} \\ =& \frac{1}{n} \log\Big(\prod_{v \in \mathcal{P}(\mathbb{K})} \max\{|\alpha|_v, 1\}\Big), \end{aligned} \tag{4.7}$$

where $\mathcal{P}(\mathbb{K})$ denotes the set of all places of $\mathbb{K}$.

We will denote our logarithmic height in our number fields $\mathbb{K}_D$ by h_D.

Lemma 4.3.1. *Let D be in Tables 4.3 4.4. Let (x, y, p), (d_1, d_2), as above. Define*

$$c = \begin{cases} 2d_1, & \text{if } D \equiv 0 \pmod 4 \text{ and } d_2 \text{ is odd} \\ d_1, & \text{if } D \equiv 0 \pmod 4 \text{ and } d_2 \text{ is even} \\ 2d_1, & \text{if } D \equiv 1 \pmod 4 \text{ and } x \text{ is odd} \\ d_1, & \text{if } D \equiv 1 \pmod 4 \text{ and } x \text{ is even} \\ d_1, & \text{in the rest of the cases} \end{cases} \tag{4.8}$$

Then $c = l^a$, where $l \in \{2, 3, 7\}$ and $a \in \{0, 1, 2\}$. If $a \geq 1$, then l spilts in $\mathbb{K}_D = \mathbb{Q}(\sqrt{d})$, say $(l) = \mathfrak{l}\bar{\mathfrak{l}}$. Let k_0 be the smallest positive integer such that the ideal $\mathfrak{l}^{k_0}$ is principal, say $\mathfrak{l}^{k_0} = \langle \alpha_0 \rangle$. Also let

$$k = \begin{cases} 1, & \text{if } k_0 = 2 \\ 2, & \text{if } k_0 = 1 \end{cases}$$

Table 4.3: Case II: D is a unit away from square

D	$D \equiv \pmod 4$	(d_1, d_2)	c	$\mathbb{K}_D$	$\#Cl(\mathbb{K}_D)$
2	2	$(1,2)$	1	$\mathbb{Q}(\sqrt{2})$	1
3	3	$(1,3)$	1	$\mathbb{Q}(\sqrt{3})$	1
5	1	$(1,5)$	1 or 2	$\mathbb{Q}(\sqrt{5})$	1
8	0	$(1,8)$	1	$\mathbb{Q}(\sqrt{2})$	1
10	2	$(1,10)$	1	$\mathbb{Q}(\sqrt{10})$	2
15	3	$(1,15)$	1	$\mathbb{Q}(\sqrt{15})$	2
17	1	$(1,17)$	1 or 2	$\mathbb{Q}(\sqrt{17})$	1
24	0	$(1,24)$	1	$\mathbb{Q}(\sqrt{6})$	1
26	2	$(1,26)$	1	$\mathbb{Q}(\sqrt{26})$	2
35	3	$(1,35)$	1	$\mathbb{Q}(\sqrt{35})$	2
37	1	$(1,37)$	1 or 2	$\mathbb{Q}(\sqrt{37})$	1
48	0	$(1,48)$	1	$\mathbb{Q}(\sqrt{3})$	1
50	2	$(1,50)$	1	$\mathbb{Q}(\sqrt{2})$	1
63	3	$(1,63)$	1	$\mathbb{Q}(\sqrt{7})$	1
		$(3,7)$	3		
65	1	$(1,65)$	1 or 2	$\mathbb{Q}(\sqrt{65})$	2
80	0	$(1,80)$	1	$\mathbb{Q}(\sqrt{5})$	1
82	2	$(1,82)$	1	$\mathbb{Q}(\sqrt{82})$	4
99	3	$(1,99)$	1	$\mathbb{Q}(\sqrt{11})$	1

Then there exist $\lambda \in \mathbb{K}_D$, $r \in \{k, 2, \ldots, p+k-1\}$, *such that*

$$\frac{x - q\sqrt{d}}{x + q\sqrt{d}} = \alpha^k \overline{u}^{2r} \lambda^p, \tag{4.9}$$

where u *is a fundamental unit of* $\mathbb{K}_D$ *such that* $\log(\overline{u}) = \max\{\log(|u|), \log(|\overline{u}|)\}, \alpha = (\overline{\alpha_0}/\alpha_0)^a$, *with* $\alpha < 1$ *and positive,* $\lambda < 1$ *and also positive, and*

$$\mathrm{h}_D(\alpha) = \frac{1}{2}\Big(\log(d_\alpha) - \log(\alpha)\Big),$$
$$\mathrm{h}_D(\lambda) = \frac{1}{2}\Big(\log(d_y) - \log(\lambda)\Big),$$

where $d_\alpha \mid c^{k_0}$ *and* $d_y \mid y$.

Table 4.4: Case III: D is neither a square or a unit away from a square

D	$D \equiv \pmod 4$	(d_1, d_2)	c	$\mathbb{K}_D$	$\#Cl(\mathbb{K}_D)$
20	0	$(1, 20)$	1	$\mathbb{Q}(\sqrt{5})$	1
21	1	$(1, 21)$	1 or 2	$\mathbb{Q}(\sqrt{21})$	1
29	1	$(1, 29)$	1 or 2	$\mathbb{Q}(\sqrt{29})$	1
33	1	$(1, 33)$	1 or 2	$\mathbb{Q}(\sqrt{33})$	1
41	1	$(1, 41)$	1 or 2	$\mathbb{Q}(\sqrt{41})$	1
45	1	$(1, 45)$	1 or 2	$\mathbb{Q}(\sqrt{5})$	1
52	0	$(1, 52)$	1	$\mathbb{Q}(\sqrt{13})$	2
55	3	$(1, 55)$	1	$\mathbb{Q}(\sqrt{55})$	2
57	1	$(1, 57)$	1 or 2	$\mathbb{Q}(\sqrt{57})$	1
68	0	$(1, 68)$	1	$\mathbb{Q}(\sqrt{17})$	1
		$(2, 17)$	4		
72	0	$(1, 72)$	1	$\mathbb{Q}(\sqrt{2})$	1
73	1	$(1, 73)$	1 or 2	$\mathbb{Q}(\sqrt{73})$	1
75	3	$(1, 75)$	1	$\mathbb{Q}(\sqrt{75})$	1
77	1	$(1, 77)$	1 or 2	$\mathbb{Q}(\sqrt{77})$	1
84	0	$(1, 84)$	1	$\mathbb{Q}(\sqrt{21})$	1
85	1	$(1, 85)$	1 or 2	$\mathbb{Q}(\sqrt{85})$	1
90	2	$(1, 90)$	1	$\mathbb{Q}(\sqrt{10})$	2
		$(3, 10)$	3		
97	1	$(1, 97)$	1 or 2	$\mathbb{Q}(\sqrt{97})$	1
98	2	$(1, 98)$	1	$\mathbb{Q}(\sqrt{7})$	2
		$(7, 2)$	7		

Proof. We begin with the factorization

$$(x + q\sqrt{d})(x - q\sqrt{d}) = y^p.$$

First we will show that any prime divisor l of y splits in $\mathbb{K}_D$. Suppose otherwise, then we may write $\langle l \rangle = \mathfrak{l}$ or $\langle l \rangle = \mathfrak{l}^2$ for some prime ideal $\mathfrak{l}$ satisfying $\bar{\mathfrak{l}} = \mathfrak{l}$. If $p = 2r + 1$ then clearly $\mathfrak{l}^r$ divides both factors on the left-hand side above and so divides $2q\sqrt{d}$. This is impossible in view of the fact that we are assuming $p \geq 10^3$ and $1 \leq D \leq 100$. Thus, we have shown that every prime divisor l of y splits in our number field $\mathbb{K}_D$. Put

$$y = \prod_{i \in I} l_i^{a_i} \text{ and } (l_i) = \mathfrak{l}_i \bar{\mathfrak{l}}_i, i \in \{1, \ldots, r\},$$

then we have

$$(x + q\sqrt{d}) = \prod_{i \in I} (\mathfrak{l}_i^{b_i} \bar{\mathfrak{l}}_i^{c_i}) \text{ and } (x - q\sqrt{d}) = \prod_{i \in I} (\mathfrak{l}_i^{c_i} \bar{\mathfrak{l}}_i^{b_i}),$$

with $b_i + c_i = pa_i$, for all $i \in I$ and we assume (for ease of notation) that $b_i \geq c_i$ for all i. Then, clearly,

$$\mathfrak{d} := \gcd\left(\langle x + q\sqrt{d} \rangle, \langle x - q\sqrt{d} \rangle\right) = \prod_{i \in I} (\mathfrak{l}\bar{\mathfrak{l}}_i)^{c_i} = \prod_{i \in I} \langle l_i \rangle^{c_i}.$$

This shows that $\mathfrak{d} = \langle c \rangle$, where $c \in \mathbb{Z}$. We will now calculate c and verify that its value is in agreement with (4.8). From the definition of $\mathfrak{d}$ we see that $c \mid 2x$ and that $c \mid 2\sqrt{d}q$. However, by our definition of signature, $\gcd(x^2, D) = d_1^2$, it follows that $c^2 \mid 4d_1^2$ and so $c \mid 2d_1$. However, $d_1 \mid x$ and $d_1 \mid q$. Hence, $d_1 \mid \mathfrak{d}$ and so $d_1 \mid c$. Thus $c = d_1$ or $c = 2d_1$. We note the following cases:

I : $D \equiv 2, 3 \pmod 4$, so $2 \nmid y$ and then we have $2 \nmid c$, therefore $c = d_1$.

II : $D \equiv 1 \pmod 4$. Consequently we have that $d \equiv 1 \pmod 4$. Now we also have that $D = d_1^2 d_2$, $x = d_1 t$, where $\gcd(d_2, t) = \gcd(d_1, d_2) = 1$.

(i) If x is even, then t is even, thus $2 \nmid y$ and we have that $c = d_1$.

(ii) If x is odd, then t is also odd. So define $d_3 = q/d_1$, which is still a integer and an odd number. We have that $d_2 = d_3^2 d$. So we have

$$\langle c \rangle = \mathfrak{d} = 2d_1 \gcd\Big(\Big(\frac{t + d_3\sqrt{d}}{2}\Big), \Big(\frac{t - d_3\sqrt{d}}{2}\Big)\Big),$$

since $\frac{t \pm d_3\sqrt{d}}{2} \in \mathfrak{O}_D$, we have that $c = 2d_1$.

III: $D \equiv 0 \pmod 4$. We have that d_2 is even if and only if x is odd, if and only if y is odd. So if d_2 is even then we have that $c = d_1$. If d_2 is odd, then t is also odd too, and using the same argument as in item II, part (ii), we have that $c = 2d_1$.

This proves that c satisfies (4.8). Looking at Tables 4.3 and 4.4, we see the possible values of c for the values of D we are looking at, and we see that $c = l^a$, where $a \in \{0, 1, 2\}$ and $l \in \{2, 3, 7\}$. Let $j \in I$ be such that $c = l_j^{c_j}$, thus, $c_i = 0$ for all $i \neq j$. Then

$$(x + q\sqrt{d}) = \bar{\mathfrak{l}}_j^{c_j} . \mathfrak{l}_j^{b_j} . \prod_{j \neq i} \mathfrak{l}_i^{pa_i},$$

whence

$$(x + q\sqrt{d}) = (\bar{\mathfrak{l}}_j . \mathfrak{l}_j^{-1})^{c_j} . \prod_{i \in I} \mathfrak{l}_i^{pa_i} = (\mathfrak{a}\bar{\mathfrak{a}}^{-1})\mathfrak{g}^p,$$

where $\mathfrak{a}$ and $\mathfrak{g}$ are integral idelas with $\mathfrak{a} = \bar{\mathfrak{l}}^{c_j}, \mathcal{N}(\mathfrak{a}) = l_j^{c_j} = c$, therefore $c_j = a, \mathcal{N}(\mathfrak{g}) = y$, and $\mathcal{N}$ denotes the norm. Thus, as fractional ideals,

$$\Big(\frac{x - q\sqrt{d}}{x + q\sqrt{d}}\Big) = (\bar{\mathfrak{a}}\mathfrak{a}^{-1})^2 (\bar{\mathfrak{g}}\mathfrak{g}^{-1})^p.$$

Now we define k_0, k, α_0 as in the statement of the lemma. From the Tables 4.3 and 4.4, if $c \neq 1$, then Thus, $\mathfrak{a}^{k_0} = \langle \alpha_0^a \rangle$, with $k_0 \in \{1, 2\}$, due to the class

numbers of the our number fields $\mathbb{K}_D$ and the value of our c (see tables 4.3 and 4.4) and we have the following relation, between ideals,

$$(x + q\sqrt{d}) = (\mathfrak{a}/\overline{\mathfrak{a}})\mathfrak{g}^p = \mathfrak{a}^2(\mathcal{N}(\mathfrak{a}))^{-1}\mathfrak{g}^p = \alpha_0^{ak}c^{-1}\mathfrak{g}^p.$$

However, p is a prime greater or equal to 10^3, certainly not dividing the class number. This shows that $\mathfrak{g}$ is also principal, $\mathfrak{g} = \langle\lambda_0\rangle$ say, where λ_0 is an algebraic integer chosen so that the following equality of elements of $\mathbb{K}_D$ holds

$$x + q\sqrt{d} = \alpha_0^{ak}c^{-1}u^r\lambda_0^p$$

with $\mathcal{N}(\alpha_0) = c^{k_0}$, u a fundamental unit of $\mathbb{K}_D$, satisfying the conditions on the statement of the Lemma, with $r \in \{k, 2, \ldots, p + k - 1\}$ and $\mathcal{N}(\lambda_0) = y$. Put $\alpha = \overline{\alpha}_0/\alpha_0$ and $\lambda = \overline{\lambda}_0/\lambda_0$.

About having $\alpha < 1$, if α_0^a generates $\mathfrak{a}^{k_0}$, then $\alpha_0^a u^s$ also generates it, for any integer s. So we have $\tilde{\alpha} = \overline{\alpha}_0^a\overline{u}^s/\alpha_0^a u^s = \alpha\overline{u}^{2s}$. So we want $\tilde{\alpha} < 1$, that is $\log(\alpha) + 2s\log(\overline{u}) < 0$, which is equivalent to have

$$s < -\frac{\log(\alpha)}{2\log(\overline{u})}. \tag{4.10}$$

Therefore we choose

$$s = \Big\lfloor -\frac{\log(\alpha)}{2\log(\overline{u})}\Big\rfloor.$$

In order to have $\lambda < 1$, Now we multiply $\alpha_0^a u^s$ by u^t, where t is an integer. As before we have that $\alpha_0^a u^{s+t}$ generates the ideal $\mathfrak{a}^{k_0}$. So from (4.9), we have that $\alpha^k\overline{u}^{2(sk+tk+r)}\lambda^p < 1$, that is equivalent to have

$$\lambda < \Big(\frac{1}{\alpha^k\overline{u}^{2(ks+kt)}}\Big)^{1/p}.$$

So we just need to consider $\frac{1}{\alpha^k\overline{u}^{2(sk+tk+r)}} < \frac{1}{\alpha^k\overline{u}^{2(sk+tk+k)}} < 1$, assuming that $r \geq 1$. But this is equivalent to have that $-k\log(\alpha) - (2sk + 2tk + 2k)\log(\overline{u}) < 0$,

that is

$$-\frac{\log(\alpha)}{2\log(\overline{u})} - 1 - s < t. \tag{4.11}$$

So combining the information of (4.10) and (4.11), we define

$$t = \left\lfloor -\frac{\log(\alpha)}{2\log(\overline{u})} - 1 - s \right\rfloor + 1,$$

our new α_0 to be $\alpha_0 u^{t+s}$ and our new α to be $\alpha\overline{u}^{2(t+s)}$ and we will have

$$0 < \alpha, \lambda < 1.$$

To verify that our new α is less than one, we just need to verify that

$$t + s \leq -\frac{\log(\alpha)}{2\log(\overline{u})}.$$

Given what we have seen before, we have Now

$$\begin{aligned} t &= \left\lfloor -\frac{\log(\alpha)}{2\log(\overline{u})} - 1 - s \right\rfloor + 1, \\ &\leq \left\lfloor -\frac{\log(\alpha)}{2\log(\overline{u})} - 1 - \left\lfloor -\frac{\log(\alpha)}{2\log(\overline{u})} \right\rfloor \right\rfloor + 1, \\ &\leq 0. \end{aligned}$$

Therefore $t + s \leq s \leq -\frac{\log(\alpha)}{2\log(\overline{u})}$, by the definition of s.

For the rest of the proof, the statements concerning the heights of α and λ, just use the definition of a logarithmic height, what we have just proved now and the lemma 4.3.2 below as the fact that $\alpha^{-1} = \overline{\alpha}$ and $\lambda^{-1} = \overline{\lambda}$. **QED**

Lemma 4.3.2. *Let $\mathbb{K}$ be a number field of degree 2 over $\mathbb{Q}$, let α be an algebraic number such that $\alpha = \overline{\alpha}_0/\alpha_0$, where α_0 is an algebraic integer. Let $P(X) = a_2X^2 + a_1X + a_0$ be the minimal polynomial of α over $\mathbb{Z}[X]$, then $a_2 \mid \mathcal{N}(\alpha_0)$. Also, we have that $h(\alpha) = h(\overline{\alpha})$.*

Proof. Let $\mathbb{K} = \mathbb{Q}(\sqrt{m})$, where m is a square-free integer. Let $\alpha = \overline{\alpha}_0/\alpha_0$, then $\overline{\alpha} = \alpha_0/\overline{\alpha}_0$. Let $\tilde{P}(X)$ be the minimal polynomial of α over $\mathbb{Q}[X]$, then it is a well know fact that

$$\tilde{P}(X) = (X - \alpha)(X - \overline{\alpha}) = X^2 - (\alpha + \overline{\alpha})X + \alpha\overline{\alpha}.$$

Using only the definition of α and of a norm over a quadratic number field we easly see that first $\alpha\overline{\alpha} = \frac{\overline{\alpha}_0}{\alpha_0}\frac{\alpha_0}{\overline{\alpha}_0} = 1$ and secondly

$$\alpha + \overline{\alpha} = \frac{\overline{\alpha}_0}{\alpha_0} + \frac{\alpha_0}{\overline{\alpha}_0} = \frac{\overline{\alpha}_0^2 + \alpha_0^2}{\alpha_0\overline{\alpha}_0} = \frac{\overline{\alpha}_0^2 + \alpha_0^2}{\mathcal{N}(\alpha_0)}$$

. Thus we conclude that $P(X) = a_2.\tilde{P}(X)$, where $a_2 \mid \mathcal{N}(\alpha_0)$.

QED

We are now ready to write down the linear form in logarithms, Define

$$\Lambda := \log\left(\frac{x - q\sqrt{d}}{x + q\sqrt{d}}\right), \tag{4.12}$$

where we consider the real logarithm. Now we separate in two cases:

(I) $c = 1$;

(II) $c \neq 1$.

In case (I) our α_0 can be chosen to be equal to 1, for $\langle c\rangle = \langle 1\rangle = \mathfrak{O}_D$, that is already a principal ideal, and so (4.9) can be rewritten in the following way

$$\frac{x - q\sqrt{d}}{x + q\sqrt{d}} = \overline{u}^{2r}\lambda^p,$$

and then our linear form in logarithms (4.12) turns out to be a linear form in two logarithms, with the following expression:

$$\Lambda_2 := 2r\log(\overline{u}) + p\log(\lambda). \tag{4.13}$$

In case (II) there is nothing to change about the equality (4.9). So using this last equality we have that our linear form in logarithms (4.12) is a linear form in three logarithms with the following expression

$$\Lambda_3 := k\log(\alpha) + 2r\log(\overline{u}) + p\log(\lambda). \tag{4.14}$$

By our choices in the previous Lemma we have that $\alpha, \overline{u}, \lambda$ are all positive. Now let us take a look at the logarithmic height of λ.

We have chosen λ to be positive and less than one. By (4.9) we have that

$$\lambda^p < \frac{1}{\alpha^k \overline{u}^{2r}}.$$

Applying logarithms in both sides, we have that

$$\log(\lambda) < \frac{1}{p}\Big(- k\log(\alpha) - 2r\log(\overline{u})\Big). \tag{4.15}$$

Now, considering our bounds for x, considering it positive, we have that

$$\frac{x - q\sqrt{d}}{x + q\sqrt{d}} \geq \frac{10^3 - q\sqrt{d}}{10^3 + q\sqrt{d}},$$

due to the fact that the function $f(x) = \frac{x-a}{x+a}$, with $a > 0$ is always increasing when x is positive. So let $\delta = \frac{10^3 - q\sqrt{d}}{10^3 + q\sqrt{d}}$, therefore using again (4.9) and logarithms we have that

$$\frac{1}{p}\Big(\log(\delta) - k\log(\alpha) - 2r\log(\overline{u})\Big) \leq \log(\lambda). \tag{4.16}$$

.

Combining (4.15) (4.16) and the fact that $\overline{\lambda} = \lambda^{-1}$, we have that

$$\frac{1}{p}\Big(\log(\delta) - k\log(\alpha) - 2r\log(\overline{u})\Big) \leq \log(\lambda) \leq \frac{1}{p}\Big(- k\log(\alpha) - 2r\log(\overline{u})\Big)$$
$$\frac{1}{p}\Big(k\log(\alpha) + 2r\log(\overline{u})\Big) \leq \log(\overline{\lambda}) \leq \frac{1}{p}\Big(k\log(\alpha) + 2r\log(\overline{u}) - \log(\delta)\Big)$$

Therefore, using Lemma 4.3.1 we have that

$$\mathrm{h}_D(\lambda) \leq \frac{\log(y)}{2} + \frac{1}{2p}\Big(k\log(\alpha) + 2r\log(\overline{u}) - \log(\delta)\Big) \tag{4.17}$$

Just to mention that if we are in case (I), since we do not have α^k appearing in our expression for Λ_2 (see (4.13)), we have that

$$\mathrm{h}_D(\lambda) \leq \frac{\log(y)}{2} + \frac{1}{2p}\Big(2r\log(\overline{u}) - \log(\delta)\Big). \tag{4.18}$$

4.3.1 A smart bound for Λ

We start by stating a simple lemma which we will use a few times to produce bounds for linear forms in logarithms.

Lemma 4.3.3. *Let $\Delta \in \mathbb{C}$ with $|\delta - 1| \leq a$. Then*

$$|\log(\Delta)| \leq -\frac{log(1-a)}{a}|\Delta - 1|. \tag{4.19}$$

Proof. See Lemma B.2 in [Sma98]. **QED**

Let us give a first bound for Λ using basic methods.

Lemma 4.3.4. *We have*

$$\log|\Lambda| \leq -\frac{p}{2}\log y + \log(2.2q\sqrt{d}). \tag{4.20}$$

Proof. From the equality $(x - q\sqrt{d}) - (x + q\sqrt{d}) = -2q\sqrt{d}$ we easily see that

$$\left|\frac{x - q\sqrt{d}}{x + q\sqrt{d}} - 1\right| = \frac{2q\sqrt{d}}{x + q\sqrt{d}} < 2\frac{q\sqrt{d}}{|x|}.$$

The inequalities given by (4.19) and by $2q\sqrt{d}/|x| \leq 2 \times 10^{-2}$ allied to the fact that $-\log(1-a)/a \leq 2.1/2$, when $0 < a \leq 2 \times 10^{\cdot -2}$, we have that:

$$|\Lambda| < 2.1\frac{q\sqrt{d}}{|x|},$$

so that $\log|\Lambda| < -\log|x| + \log(2.1q\sqrt{d})$, using for that the bounds (4.6).

Now let us use the fact that $y^p - x^2 = -D$, so we have that

$$\left|\frac{y^p}{x^2} - 1\right| = \frac{D}{x^2} < \frac{q\sqrt{d}}{|x|}.$$

Using again the inequality given by (4.19), we see that

$$\log(y^p/x^2) \leq CD/x^2 \leq -\frac{\log(1 - q\sqrt{d}/|x|)q\sqrt{d}}{|x|},$$

where $C = -\frac{\log(1-q\sqrt{d}/|x|)|x|}{q\sqrt{d}}$. Now using the fact that $-\log(1-a) * a \leq 2\log(2.2/2.1)$, when $0 < a < 10^{-2}$ with the inequality above, we have that:

$$\log(y^p/x^2) \leq 2\log(2.2/2.1).$$

By the well-known properties of the logarithm function we have $\log(y^p/x^2) = p\log(y) - 2\log(x)$ and the result follows. **QED**

4.3.2 Matveev's Theorem: A preliminary bound for p

To bound p we use the theory of linear forms of at most three logarithms, which we have already seen in (4.13) and (4.14). We need the special case of two and of three logarithms of a theorem of Matveev, but we will present its full statement

Theorem 4.1 (Matveev). *Let $\alpha_1, \alpha_2, \ldots, \alpha_n$ be algebraic numbers, let $\mathbb{K}$ be the number field $\mathbb{Q}(\alpha_1, \alpha_2, \ldots, \alpha_n)$ of degree $\mathcal{D}$. Put $\chi = [\mathbb{R}(\alpha_1, \alpha_2, \ldots, \alpha_n) : \mathbb{R}]$. Let $b_1, b_2, \ldots, b_n$ be integers such that $b_1 \neq 0$. Define*

$$\Lambda := b_1 \log \alpha_1 + b_2 \log \alpha_2 + \cdots + b_n \log \alpha_n.$$

Suppose that we have real numbers A_j for all $j \in \{1, 2, \ldots, n\}$ satisfying

$$A_j \geq \max\{\mathcal{D}\,\mathrm{h}(\alpha_j), |\log \alpha_j|, 0.16\}.$$

Assume that $B \geq \max\{1, \max\{|b_j|A_j/A_n : \ 1 \leq j \leq n\}\}$. *For brevity we put*

$$\Omega = A_1.A_2.\ldots.A_n,$$
$$C(n) = \frac{16}{n!\chi}e^n(2n+1+2\chi)(n+2)(4(n+1))^{n+1}\Big(\frac{en}{2}\Big)^{\chi},$$
$$C_0 = \log\big(e^{4.4n+7}n^{5.5}\mathcal{D}^2\log(e\mathcal{D})\big), \quad C_1 = \max\Big\{\frac{n}{6}, 1\Big\}$$
$$W_0 = \log\big(1.5eB\mathcal{D}\log(e\mathcal{D})\big).$$

Then

$$\log|\Lambda| > -C(n)C_0C_1W_0\mathcal{D}^2\Omega. \tag{4.21}$$

Proof. For a proof of this result see [Mat00]. **QED**

We are interested when we have $\mathcal{D} = 2, \chi = 1$ and $n = 2$ or 3. For both values of n we have that $C_1 = 1$. So (4.21) becomes the following inequality,

$$\log|\Lambda| > -4C(n)C_0W_0\Omega. \tag{4.22}$$

Before making our bounds explicit, let us combine the inequalities of (4.20) and (4.22) and get an "upper bound" for p. First we start with the inequality:

$$-\frac{p}{2}\log y + \log\Big(2.2q\sqrt{d}\Big) > -4C(n)C_0W_0\Omega.$$

Working with this inequality we get the following one

$$\frac{p}{2}\log y < 4C(n)C_0W_0\Omega + \log(2.2q\sqrt{d}),$$

that is

$$p < \frac{2}{\log y}\Big(4C(n)C_0W_0\Omega + \log(2.2q\sqrt{d})\Big), \tag{4.23}$$

So we only need to find our A_j's and B that satisfy the assumptions of Theorem 4.1 and we can estimate a bound for p, using (4.23), for all the values of D that we are still considering.

Let us study each case separately. First consider case (I), $c = 1$, recall (4.13), $\Lambda_2 = 2r\log(\overline{u}) + p\log(\lambda)$. So in Matveev's Theorem we have $\alpha_1 = \overline{u}, \alpha_2 = \lambda$, $b_1 = 2r$ and $b_2 = p$. We can take

$$A_1 = \max\{\log|\overline{u}|, 0.16\},$$

since $\mathrm{h}_D(u) = \frac{1}{2}\log(\overline{u})$, for the choice of u made in Lemma (4.3.1). Now

$$A_2 \geq \max\{2\,\mathrm{h}_D(\lambda), |\log\lambda|, 0.16\}.$$

So, by what we have seen in (4.18), (4.15), with $\alpha^k = 1$, and considering the bounds for y, we can choose

$$A_2 = \log(y) + \frac{1}{p}\Big(2r\log(\overline{u}) - \log(\delta)\Big)$$

Concerning B, we want to have $B \geq \max\{1, b_1\frac{A_1}{A_2}, b_2\}$, due to our bounds (4.4), and for our choice of A_1 and A_2 we can take $B = p$.

Now we turn into the case (II), where $c \neq 1$. From what we have seen above, (4.14), we can consider $\alpha_1 = \alpha$, $\alpha_2 = \overline{u}$, $\alpha_3 = \lambda$, $b_1 = 1$, $b_2 = 2r$ and $b_3 = p$. Considering what we have seen in the Lemma 4.3.1 and on (4.17), we can choose

$$A_1 = \max\{k_0\log(c) + \log|\overline{\alpha}|, 0.16\},$$

$$A_2 = \max\{\log|\overline{u}|, 0, 16\}, \text{ and}$$

$$A_3 = \log(y) + \frac{1}{p}\Big(k\log(\alpha) + 2r\log(\overline{u}) - \log(\delta)\Big).$$

And we also assume that $B = p$, just taking account how we have define A_1, A_2, A_3 and the bounds (4.4). Now we are ready to apply Theorem 4.1.

Table 4.5: Preliminaries bounds for p

D	c	n	p_0
2	1	2	16 588 404 257
3	1	2	26 032 647 527
5	1	2	8 558 182 513
	2	3	10^3
8	1	2	16 588 404 257
10	1	2	37 745 048 087
15	1	2	43 781 188 457
17	1	2	44 566 352 087
	2	3	14 467 052 424 709
20	1	2	8 558 182 513
21	1	2	31 758 311 327
	2	3	10^3
24	1	2	49 605 855 317
26	1	2	50 123 053 649
29	1	2	33 648 055 843
	2	3	10^3
33	1	2	93 108 842 791
	2	3	39 428 986 936 327
35	1	2	54 451 041 013
37	1	2	54 818 536 139
	2	3	10^3
41	1	2	103 476 735 361
	2	3	49 550 951 449 781
45	1	2	8 558 182 513
	2	3	10^3
48	1	2	26 032 647 527
50	1	2	16 588 404 257
52	1	2	23 313 066 299
55	1	2	137 697 171 301
57	1	2	156 672 054 503
	2	3	77 200 788 568 381
63	1	2	62 275 863 257
	3	3	24 341 940 110 029
65	1	2	62 489 936 051
	2	3	34 377 987 147 247
68	1	2	44 566 352 087
	4	3	10 626 098 324 363
72	1	2	16 588 404 257
73	1	2	234 413 560 127
	2	3	124 762 180 522 643
75	1	2	26 032 647 527
77	1	2	46 842 338 843
	2	3	10^3
80	1	2	8 558 182 513
82	1	2	65 718 762 353
84	1	2	31 758 311 327
85	1	2	47 472 286 013
	2	3	10^3
90	1	2	37 745 048 087
	3	3	5 226 185 260 435
97	1	2	309 478 531 499
	2	3	321 528 361 566 911
98	1	2	16 588 404 257
	7	3	5 825 508 008 693
99	1	2	68 508 206 209

Proposition 4.3.1. *Suppose that D is one of the values in tTables 4.3 and 4.4 and (x, y, p) is a solution to* (3.1)*, with bounds given in* (4.6)*,* (4.4) *and* (4.5)*. Then for $p \geq p_0$ given in Table 4.5, the equation* (3.1) *does not have any solution for the values D in table 4.4 and for the values D in Table 4.3, the only solution that there is for $p \geq p_0$ is the one where $|y| = 1$.*

Proof. From (4.23) we have that

$$p \leq \frac{\tilde{C}_1 + \tilde{C}_2}{\log(y)},$$

where $\tilde{C}_1 = 2C(n)C_0W_0\mathcal{D}^2\Omega$ and $\tilde{C}_2 = \log(2.2q\sqrt{d})$ As we have seen above, in both cases (I) and (II) we have that $B = p$, and since W_0 depends on B, we can rewrite $\tilde{C}_1$ as $\tilde{C}_1 = \tilde{C}_3 \log(\tilde{C}_4 p)$, where $\tilde{C}_4$ is easily computable.

Now we consider the values A_1, A_2 and A_3 (when necessary) as we have defined above. We consider $B = p$. When $c \neq 1$, A_1 depends on α, as does A_3 in case (II), but it is possible to calculate α for each case, verifying the hypothesis of the Lemma 4.3.1, that c must split over $\mathbb{K}_D$, for c is going to be a power of a prime. The value A_2 (resp. A_3) depends on y as in case (I) (resp. case (II)), which means that Ω, in both cases, will depend on y. Therefore, we can rewrite $\tilde{C}_3$ as follows $\tilde{C}_3 = \tilde{C}_5(\log(y)/2 + \tilde{C}_6)$, where now $\tilde{C}_5$ and $\tilde{C}_6$ are easily computable. So as we have seen before, applying Matveev's Theorem, we get the bound (4.23), and considering what we have seen right now, we have that

$$p \leq \left(\tilde{C}_5(\log(y)/2 + \tilde{C}_6)\log(\tilde{C}_4 p) + \tilde{C}_2\right)/\log(y) \tag{4.24}$$

Now since we have that $y \geq (\sqrt{p} - 1)^2$, (4.24) implies:

$$p \leq \left(\tilde{C}_5(\log(\sqrt{p} - 1) + \tilde{C}_6)\log(\tilde{C}_4 p) - \tilde{C}_2\right)/2\log(\sqrt{p} - 1)$$

Therefore we are looking for a zero of the function

$$f(X) = X - \left(\tilde{C}_5(\log(\sqrt{X} - 1) + \tilde{C}_6)\log(\tilde{C}_4 X) - \tilde{C}_2\right)/2\log(\sqrt{X} - 1)$$

If x_0 is the zero of $f(X)$ we take $p_0 = \max\{p \text{ a prime} | p \leq \lfloor x_0 \rfloor + 1\}$. For the computation of every constant mentioned above we wrote a simple program in MAGMA, that gives us also the bounds, $p \leq p_0$, that are presented on table 4.5. **QED**

Remark. As we can see in Table 4.5, we have that in some cases $p_0 = 10^3$. This happens when $c = 2$, and for $D = 5, 21, 29, 37, 45, 77$ and 85, because in these cases, 2 does not split in $\mathfrak{O}_D$, which contradicts what we have seen in Lemma 4.3.1. Therefore in this cases we have that our bound for p is 10^3.

4.3.3 Linear forms in two logarithms

In this and in the next section we will consider separately the linear forms in two logarithms Λ_2 and in three logarithms Λ_3. We will try to improve the bounds that we have from applying Matveev's theorem 4.1. For that purpose we will use two of the main results of Mignotte's paper [Mig08]

Let us begin with case (I), where Λ_2 is a linear form in two logarithms. For the case of linear forms in two logarithms, there are quite few papers on the subject, more than in the case of linear forms in three logarithms, and one of the best known papers is the paper of Laurent, Mignotte and Nesterenko [LMN95], where we are provided with results that, when applied to our linear form Λ_2 can help us to estimate a good bound for p. Instead we will use Theorem 3 of [Mig08], that provides a sharper bound for p than the main results of [LMN95]. And in terms of practice, turns out to be easier. Before moving on to the statement and application of the mentioned result, just for the sake of completeness, there is a new paper of Laurent [Lau08], that provies an even sharper bound than Theorem 3 of [Mig08], but its philosophy and its pratical application are very similar to the

results of [LMN95].

Let α_1, α_2 be two non-zero algebraic numbers, and let $\log \alpha_1$ and $\log \alpha_2$ be any determinations of their logarithms. We consider here the linear form

$$\Lambda = b_2 \log \alpha_2 - b_1 \log \alpha_1,$$

where b_1 and b_2 are positive integers. Without loss of generality, we suppose that the absolute values $|\alpha_1|$ and $|\alpha_2|$ are ≥ 1. Put

$$\mathcal{D} = [\mathbb{Q}(\alpha_1, \alpha_2) : \mathbb{Q}]/[\mathbb{R}(\alpha_1, \alpha_2) : \mathbb{R}].$$

Suppose further more that the number α_1 is not a root of unity.

Proposition 4.3.2. *Consider $\Lambda, b_1, b_2, \alpha_1, \alpha_2$ and $\mathcal{D}$ as above. Let a_1, a_2, h, k be positive real numbers, and r a real number > 1. Put $\rho = log(r)$ and suppose that*

$$h \geq \max\{1, 1.5\rho, \mathcal{D}\Big(\log\left(\frac{b_1}{a_2} + \frac{b_2}{a_1}\right) + \log\rho + f(K)\Big) + 0.0262\},$$

$$a_i \geq \max\{4, 2.7\rho, r|\log\alpha_i| - \log|\alpha_i| + 2\mathcal{D}\,\mathrm{h}(\alpha_i)\}, \quad (i = 1, 2),$$

$$a_1 a_2 \geq 20\rho^2,$$

where

$$f(x) = \log\frac{(1+\sqrt{x-1})\sqrt{x}}{x-1} + \frac{\log x}{6x(x-1)} + \frac{3}{2} + \log\frac{3}{4} + \frac{\log\frac{x}{x-1}}{x-1}$$

and

$$L = 2 + \lfloor 2h/\rho \rfloor \geq 5, K = 1 + \lfloor kLa_1a_2 \rfloor.$$

Then we have the lower bound

$$\log|\Lambda| \geq -\rho k L^2 a_1 a_2 - \max\{\rho(L-0.5) + \log\big(L^2(1+\sqrt{k})\big)a_2, \mathcal{D}\log 2\},$$

provided k satisfies $k \leq 2.2\rho^{-2}$ and

$$kU - V\sqrt{k} - W \geq 0,$$

with

$$U = (L-1)\rho - h,\ V = L/3,\ W = \frac{1}{4}\Big(\frac{L}{a_2} + \frac{1}{a_1}\Big).$$

Proof. See section 4.4 of [Mig08] for the proof of this proposition. **QED**

Before showing how to apply this result to our case, let us first give some considerations about the choice of some parameters.

Following the discussion in section 4.3 of [Mig08] we see that we need to choose a k such that

$$\frac{4}{9\rho^2} \leq k \leq \frac{2.2}{\rho^2},$$

and this will satisfy the conditions mentioned in Proposition 4.3.2. So we just need to choose a positive real number k_0 such that $40 \leq k_0 \leq 1980$ and

$$k = \frac{k_0}{90}\rho^{-2}.$$

From the statement of the proposition, we see that h is in some way dependent on K and K is also dependent of h. To overcome this problem, we just need to notice that the function $f(x)$ mentioned in the Proposition, is decreasing, so we can choose a value $K_h \geq 5$ and set

$$h = \max\left\{1, 1.5\rho, \mathcal{D}\Big(\log\left(\frac{b_1}{a_2} + \frac{b_2}{a_1}\right) + \log\rho + f(K_h)\Big) + 0.0262\right\}.$$

Then we just need to verify that $K \geq K_h$, which in some cases might not happen, but then we simply adjust K_h to the value of K given in the computation and it will work out.

Now let us see how to apply Proposition 4.3.2 to our case, Λ_2. By our choice of λ, we have that $0 < \lambda < 1$, in order to apply Proposition 4.3.2, we rewrite Λ_2 in the following way

$$\Lambda_2 := 2r\log(\overline{u}) - p\log(\overline{\lambda}),$$

due to the fact that $\lambda^{-1} = \overline{\lambda}$. Therefore we have the following identifications

$$\alpha_1 = \overline{\lambda},\ b_1 = p,\ \alpha_2 = \overline{u} \text{ and } b_2 = 2r.$$

First of all we fix $\tilde{r} > 1$, then for each $i \in \{1, 2\}$, we can compute a_i easily, that turn out to be

$$a_1 = \max\{4, 2.7\rho, 2\log y + \frac{\tilde{r}-1}{p}(2r\log\overline{u} - \log\delta)\},$$
$$a_2 = \max\{4, 2.7\rho, (\tilde{r}+1)\log\overline{u}\},$$

where δ is as in section 4.3, in the discussion following Lemma 4.3.1. Let k_0 and k be as before. We choose h as we have stated before, choosing $K_h = 5$. Since a_1 is dependent on y and r, we choose $y = 10^3$ and $r = p$, the maximum value permitted for r. And since both a_1 and a_2 are dependent on p, we choose $p = p_0$, the value given in Table 4.5.

Then we compute L and K as in the statement of the proposition. If $L \geq 5$, then we compute

$$C(L, \rho, k, a_1, a_2) = \rho k L^2 a_1 a_2 - \max\{\rho(L - 0.5) + \log\left(L^2(1+\sqrt{k})\right)a_2, \mathcal{D}\log 2\}.$$

Then using a similar argument to the one presented after the statement of Matveev's Theorem, we have that

$$p \leq \frac{2}{\log y}\Big(C(L, \rho, k, a_1, a_2) + \log 2.2q\sqrt{d}\Big).$$

We can repeat this process several times, till we find a lower bound for p that cannot be improved, and for each iteration of this process, we might choose different K_h and different $\tilde{r}$ and also a different k_0, though our computations revealed that the best result is always obtained for $k_0 = 40$.

Let us give an example of how it works.

Table 4.6: Bounds for p when $D = 72$.

j	$\tilde{r}$	k_0	K_h	K	L	h	p
1	9.159	40	1225	1230	44	47.616	29 017
2	9.242	40	560	562	20	21.123	6 047
3	9.465	40	480	483	17	17.981	4 463
4	8.821	40	465	467	17	17.417	4 177
5	8.686	40	460	464	17	17.294	4 133
6	8.665	40	460	464	17	17.274	4 111

Example 4.3.1. Consider $D = 72$, following the notation of these notes, we have that $\mathbb{K}_D = \mathbb{Q}(\sqrt{2})$. From Matveev's Theorem, we have as first bound for p, 16 588 404 257. We choose $\overline{u} = 1 + \sqrt{2}$, therefore we choose a_1, a_2 the following equalities

$$a_1 = \max\{4, 2.7\rho, 2\log y + \frac{\tilde{r}-1}{p}(1.7268 \times r + 0.003)\},$$

$$a_2 = \max\{4, 2.7\rho, 0.8814 \times (\tilde{r}+1)\}.$$

Now choosing convenient k_0 and $\tilde{r}$, taking $y = 4 \times 10^3$ and with the identifications made above at the discussion, the bounds we get at each iteration of this process are given on table 4.6, where j means the j^{th}-iteration.

So for $D = 72$ and $p \geq 4111$ we know that equation (3.1) does not have any integral solution.

For the rest of the cases we have the following Proposition:

Proposition 4.3.3. *Let D be one of the values in Table 4.5, and suppose $c = 1$, where c is defined in Lemma 4.3.1. Then for D a value in Table 4.4 the equation* (3.1) *does not have any solution for $p \geq p_0$, where p_0 is given in Table 4.7. When D is a value in Table 4.3 , the equation* (3.1) *does not have any non-trivial solution for $p \geq p_0$, where p_0 is given in Table 4.7, meaning, that the only solution is the trivial one, when $|y| = 1$.*

Table 4.7: Bounds for p using linear forms in two logarithms

D	$C(c)$	i	p_0
2	4	6	4 111
3	7.7	6	7 793
5	1.7	5	1 759
8	4	6	4 111
10	13.1	7	13 291
15	16.3	6	16 433
17	16.7	7	16 843
20	1.7	5	1 759
21	10.3	6	10 357
24	19.5	7	19 687
26	19.8	7	19 979
29	11.1	7	11 273
33	48.1	7	48 259
35	22.4	7	22 483
37	22.6	7	22 709
41	55.9	7	56 003
45	1.7	7	1 741
48	7.7	6	7 703

D	$C(c)$	i	p_0
50	4	6	4 111
52	6.6	6	6 661
55	83.3	7	83 389
57	99.5	7	99 667
63	27.1	6	27 253
65	27.2	7	27 367
68	16.7	7	16 843
72	4	6	4 111
73	171.9	7	172 049
75	7.7	6	7 793
77	18	7	18 097
80	1.7	5	1 759
82	29.3	7	29 423
84	10.2	6	10 369
85	18.3	7	18 461
90	13.1	7	13 291
97	248.5	8	248 639
98	4	6	4 111
99	31.1	7	31 223

Proof. We start by fixing $1 < \tilde{r} \leq 100$ and $40 \leq k_0 \leq 198$. We define then

$$\rho = \log \tilde{r}, \quad k = \frac{k_0}{90\rho^2}.$$

We set now $K_h = 5$, and we define the following quantities

$$h = \max\{1, 1.5\rho, \mathcal{D}\Big(\log(\frac{b_1}{a_2} + \frac{b_2}{a_1}) + \log\rho + f(K_h)\Big) + 0.0262\},$$
$$a_1 = \max\{4, 2.7\rho, 2\log y + \frac{\tilde{r}-1}{p}(2r\log\overline{u} - \log\delta)\},$$
$$a_2 = \max\{4, 2.7\rho, (\tilde{r}+1)\log\overline{u}\},$$

where f is the function defined on proposition 4.3.2, $b_1 = p$ and $b_2 = 2p$, where p is equal to the bound that we got from using Matveev's Theorem (see 4.5). We choose $y = C(c)10^3$, with $C(c)$ given in Table 4.7, due to the fact that for higher values of y our bounds for p would be lower, as we said before, and $C(c)$ is a constant that depends on the value of c (see Lemma 4.3.1). We compute L and K as in Proposition 4.3.2, and if $a_1 a_2 \geq 20\rho^2$ then we define

$$p_0 := \frac{2}{\log y}\left(C(L, \rho, k, a_1, a_2) + \log(2.2q\sqrt{d})\right).$$

And we iterate this process while $p_0 < p$, and in each new iteration we take p as equal to the p_0 of the previous iteration. When finished, we can re-run the computation, adjusting the values of K_h closer to the values of K given in each iteration, so that the bounds can be better. Writing a program that implements this process on `MAGMA`, we were able to compute the bounds given in Table 4.7. **QED**

Proposition 4.3.4. *For the following values of D, the equation* (3.1) *with $p \geq 7$ does not have any solution.*

$$20, 21, 29, 45, 52, 55, 72, 75, 77, 84, 85.$$

Proof. From what we have seen in Table 4.2, these values only have a linear form in two logarithms. So using the bounds we have in Table 4.7 combined with Methods I, II and III from chapter 3, we can easily eliminate all exponents for all values of D of the list above, except the following cases:

$$(D, p) = \quad (29, 7),\ (55, 7),\ (75, 7).$$

Using Thue equations we were able to show there are no solutions for these particular cases. The proposition follows. **QED**

4.3.4 Linear forms in three logarithms

Now we turn in to the case (II), where our linear form is a linear form in three logarithms Λ_3. We shall apply the following theorem.

Theorem 4.2. *We consider three non-zero algebraic numbers α_1, α_2 and α_3, which are all real and > 1 or all complex of modulus one and all $\neq 1$.*

Moreover, we assume that

$$\begin{cases} \text{either } \alpha_1, \alpha_2 \text{ and } \alpha_3 \text{ are multiplicatively independent, or} \\ \text{two are multiplicatively independent, the third one is a root of unity } \neq 1. \end{cases} \tag{M}$$

Let

$$\mathcal{D}_1 = [\mathbb{Q}(\alpha_1, \alpha_2, \alpha_3) : \mathbb{Q}],\ \mathcal{D}_2 = [\mathbb{R}(\alpha_1, \alpha_2, \alpha_3) : \mathbb{R}] \text{ and}$$
$$\mathcal{D} = \mathcal{D}_1/\mathcal{D}_2.$$

We also consider three positive rational integers b_1, b_2, b_3 with $\gcd(b_1, b_2, b_3) = 1$ and the linear form

$$\Lambda := b_2 \log \alpha_2 - b_1 \log \alpha_1 - b_3 \log \alpha_3,$$

where the logarithms of the α_i are arbitrary determinations of the logarithm, but which are all real or all purely imaginary. We assume that

$$0 < |\Lambda| < \pi \mathcal{D}_1^{-1.6}.$$

And we assume also that

$$b_2 |\log \alpha_2| = b_1 |\log \alpha_1| + b_3 |\log \alpha_3| \pm |\Lambda|.$$

We put

$$e_1 = \gcd(b_1, b_2), \quad e_3 = \gcd(b_3, b_2), \quad b_2 = e_1 b_2' = e_3 b_2''.$$

Let $K, L, R, R_1, R_2, R_3, S, S_1, S_2, S_3, T, T_1, T_2, T_3$ be positive rational integers, with

$$K \geq 3, \quad L \geq 5, \quad R > R_1 + R_2 + R_3 \quad S > S_1 + S_2 + S_3 \quad T > T_1 + T_2 + T_3.$$

Let $\rho \geq 2$ be a real number. Assume first that

$$\begin{aligned} \Big(\frac{KL}{2} + \frac{L}{4} - 1 - \frac{2K}{3L}\Big) \log \rho \geq & (\mathcal{D}+1) \log N + gL(a_1 R + a_2 S + a_3 T) \\ & + \mathcal{D}(K-1) \log b - 2 \log(e/2), \end{aligned} \tag{4.25}$$

where $N = K^2 L, e = \exp(1), g = \frac{1}{4} - \frac{N}{12RST}$,

$$b = (b_2' \nu_0)(b_2'' \eta_0) \left(\prod_{k=1}^{K-1} k! \right)^{-\frac{4}{K(K-1)}},$$

with

$$\nu_0 = \frac{R-1}{2} + \frac{(S-1)b_1}{2b_2}, \qquad \eta_0 = \frac{T-1}{2} + \frac{(S-1)b_3}{2b_2},$$

and

$$a_i \geq \rho |\log \alpha_i| - \log |\alpha_i| + 2\mathcal{D}\, \mathrm{h}(\alpha_i), \quad i = 1, 2, 3.$$

Put

$$\mu = \sqrt{(R_1+1)(S_1+1)(T_1+1)}.$$

If, for some positive real number χ*,*

(i) $(R_1+1)(S_1+1)(T_1+1) > K \times \max\{R_1+S_1+1, R_1+T_1+1, S_1+T_1+1, \chi\mu\}$,

(ii) $\#\{\alpha_1^r \alpha_2^s \alpha_2^t : 0 \le r \le R_1, 0 \le s \le S_1, 0 \le t \le T_1\} > L$,

(iii) $(R_2+1)(S_2+1)(T_2+1) > 2K^2$,

(iv) $\#\{\alpha_1^r \alpha_2^s \alpha_2^t : 0 \le r \le R_2, 0 \le s \le S_2, 0 \le t \le T_2\} > 2KL$, *and*

(v) $(R_3+1)(S_3+1)(T_3+1) > 6K^2L$,

then either

$$\Lambda' > \rho^{-KL},$$

where

$$\Lambda' = |\Lambda| \times \frac{LSe^{LS|\Lambda|/(2b_2)}}{2b_2},$$

or at least one of the following conditions hold:

$$|b_1| \le R_1 \quad \textit{and} \quad |b_2| \le S_1 \ \textit{and} \quad |b_3| \le T_1, \qquad (\mathbf{C}_1)$$

$$|b_1| \le R_2 \quad \textit{and} \quad |b_2| \le S_2 \ \textit{and} \quad |b_3| \le T_2, \qquad (\mathbf{C}_2)$$

either there exist two non-zero rational integers r_0 *and* s_0 *such that* $(\mathbf{C}_3)$

$$r_0 b_2 = s_0 b_1$$

with

$$|r_0| \le B_1 := \frac{(R_1+1)(T_1+1)}{\mathcal{M}-T_1} \quad \textit{and} \quad |s_0| \le B_2 := \frac{(S_1+1)(T_1+1)}{\mathcal{M}-T_1},$$

where

$$\mathcal{M} = \max\{R_1+S_1+1, R_1+T_1+1, S_1+T_1+1, \chi\mu\},$$

or there exist rational integers r_1, s_1, t_1 *and* t_2*, with* $r_1 s_1 \neq 0$*, such that*

$$(t_1 b_1 + r_1 b_3) s_1 = r_1 b_2 t_2, \qquad \gcd(r_1, t_1) = \gcd(s_1, t_2) = 1,$$

which also satisfy

$$|r_1 s_1| = \Delta \times B_T, \quad |s_1 t_1| \leq \Delta \times B_R, \quad |r_1 t_2| \leq \Delta \times B_S,$$

where

$$B_T := \frac{(R_1+1)(S_1+1)}{\mathcal{M} - \max\{R_1, S_1\}}, \quad B_R := \frac{(S_1+1)(T_1+1)}{\mathcal{M} - \max\{S_1, T_1\}},$$
$$B_S := \frac{(R_1+1)(T_1+1)}{\mathcal{M} - \max\{R_1, T_1\}} \quad \textit{and} \quad \delta = \gcd(r_1, s_1).$$

Moreover, when $t_1 = 0$ *we can take* $r_1 = 1$*, and when* $t_2 = 0$ *we can take* $s_1 = 1$*.*

Proof. For a proof of this result just see [Mig08]. **QED**

Now we will show how to use Theorem 4.2, as is shown in [Mig08, sec 5.2] and also in [BMS06, sec 14.2].

To apply the theorem, we consider first an integer $L \geq 5$ and real parameters $m > 0, \rho > 2$ (then we will be able to define a_i) and we put

$$K = \lfloor mLa_1a_2a_3 \rfloor, \quad ma_1a_2a_3 \geq 2.$$

To simplify the presentation, we also assume $m \geq 1$ and $a_1, a_2, a_3 \geq 1$, and put

$$R_i = \lfloor c_i a_2 a_3 \rfloor, \quad S_i = \lfloor c_i a_1 a_3 \rfloor, \quad T_i = \lfloor c_i a_1 a_2 \rfloor, \quad (i = 1, 2, 3)$$
$$R := R_1 + R_2 + R_3 + 1, \quad S := S_1 + S_2 + S_3 + 1, \quad T := T_1 + T_2 + T_3 + 1,$$

where the c_i are positive real numbers. To prove the existence of such c_i we need to satisfy conditions (i)-(v) of the Theorem 4.2. From condition (i) and (ii) we can take

$$c_1 = \max\{(\chi mL)^{2/3}, \sqrt{2mL/a}\},$$

where $a = \min\{a_1, a_2, a_3\}$. To satisfy condition (iii) and (ii) we can take

$$c_2 = \max\{2^{1/3}(mL)^{2/3}, \sqrt{m/a}L\}.$$

Finally, because of the hypothesis (M), condition (v) holds for

$$c_3 = (6m^2)^{1/3}L.$$

Remark. When $\alpha_1, \alpha_2, \alpha_3$ are multiplicatively independent then it is enough to take c_1 and c_3 as above and $c_2 = 2^{1/3}(mL)^{2/3}$.

Then we have to verify the condition (4.25). When this inequality holds, one obtains the lower bound $\Lambda' > \rho^{-KL}$ and we get

$$\log|\Lambda| > -KL\log\rho - \log(SL). \tag{4.26}$$

Now, as we have done for case (I), we consider Λ_3 in the following way

$$\Lambda_3 = 2r\log\overline{u} - \log\overline{\alpha}^k - p\log\overline{\lambda},$$

due to the fact that both α and λ are positive and less than 1. So we make the following identifications

$$\alpha_1 = \overline{\alpha}^k, \quad \alpha_2 = \overline{u}, \quad \alpha_3 = \overline{\lambda}, \tag{4.27}$$

$$b_1 = 1, \quad b_2 = 2r, \quad b_3 = p. \tag{4.28}$$

We consider $\alpha_1 = \overline{\alpha}^k$, to simplify the calculus.

For the $a_i's$ using the earlier observations about heights, we might consider

$$a_1 = (\rho+1)\log\overline{\alpha} + 2\log(c),$$

$$a_2 = (\rho+1)\log\overline{u},$$

$$a_3 = 2\log y + \frac{\rho-1}{p}(2r\log\overline{u} - \log\delta),$$

where c is as in Lemma 4.3.1.

Let us turn now to the computation of $b' = b'_2 b''_2 \nu_0 \eta_0$. We have that, due to our choice of b_1, b_2 and b_3, $d_1 = d_3 = 1$ and $b'_2 = b''_2 = b_2$, unless $b_2 = 2p$, where $d_2 = p$ and $b''_2 = 2$.

So

$$b' = \left(\frac{(R-1)b'_2}{2} + \frac{(S-1)b_1}{2e_1}\right)\left(\frac{(R-1)b''_2}{2} + \frac{(S-1)b_3}{2e_3}\right)$$

And this product will be maximized, when $r = p + k - 1$, and in this case

$$b' = \left(\frac{2(R-1)(p+k-1)}{2} + \frac{(S-1)}{2}\right)\left(\frac{2(p+k-1)(R-1)}{2} + \frac{(S-1)p}{2}\right)$$

We choose the maximum for b' so that we will have a more consistent bound for p considering each case of $r \in \{k, 2, \ldots, p+k-1\}$.

As before, when we combine the two bounds given by (4.20) and from (4.26), we have that

$$p \leq \frac{2}{\log y}\Big(KL\log\rho + \log(SL) + \log(2.2q\sqrt{d})\Big). \tag{4.29}$$

.

We only need to be careful, when conditions ($\mathbf{C}_1$), ($\mathbf{C}_2$) or ($\mathbf{C}_3$) are satisfied, when this happens we call this the degenerate case.

After finding a bound for p as given by (4.29), to verify that we are not in case ($\mathbf{C}_1$) or ($\mathbf{C}_2$), we just need to verify that

$$p > \frac{1}{2}\max\{S_1, S_2\} \quad \text{or} \quad p \geq \max\{T_1, T_2\}.$$

Let us now see what happens when condition ($\mathbf{C}_3$) is verified. For the first alternative, we need to have two rational integers r_0, s_0 such that

$$r_0 b_2 = s_0 b_1,$$

with

$$|r_0| \leq B_1, \text{ and } |s_0| \leq B_2.$$

By our linear form in three logarithms Λ_3, we have that $b_1 = 1, b_2 = 2r$, so we must have $r_0 = 1$ and $s_0 = 2r$. So we must have $2r \leq B_2$, and when this happens, then we just consider the linear form in two logarithms

$$\Lambda_3' := \log\left(\overline{u}^{2r}\alpha^k\right) - p\log\overline{\lambda}. \tag{4.30}$$

Consider now the second alternative. We must have four rational integers r_1, s_1, t_1 and t_2, with $r_1 s_1 \neq 0$ such that

$$(t_1 b_1 + r_1 b_3)s_1 = r_1 b_2 t_2, \gcd(r_1, t_1) = \gcd(s_1, t_2) = 1, \tag{4.31}$$

$$|r_1 s_1| \leq \delta \times B_T, \quad |s_1 t_1| \leq \delta \times B_R, \text{ and }, \quad |r_1 t_2| \leq \delta B_S, \tag{4.32}$$

where $\delta = \gcd(r_1, s_1)$ and the quantities B_R, B_S and B_T where defined in Theorem 4.2.

From our linear form in three logarithms Λ_3, and rewriting $r_1 = r_1'\delta$, $s_1 = s_1'\delta$ we can rewrite (4.31) in the following way,

$$(t_1 + r_1'\delta p)s_1' = r_1' 2r t_2.$$

From the conditions imposed on r_1, s_1, t_1 and t_2 in (4.31) and (4.32) we have that

$$r_1' = 1, \quad s_1' \mid 2r, \quad 2r = q's_1'$$
$$|s_1| \leq B_T, \quad |s_1' t_1| \leq B_R, \quad |t_2| \leq B_S, \text{ and}$$
$$t_1 + \delta p = q' t_2.$$

Following the discussion in section 5.3 of [Mig08] we have to distinguish three cases:

Case 1 $a = a_1$,

Case 2 $a = a_2$,

Case 3 $a = a_3$,

where $a = \min\{a_1, a_2, a_3\}$.

From the definition of the a_i's and from the discussion how to calculate the a_i's, we notice that $a_3 \geq \max\{a_1, a_2\}$, therefore there is no need to consider **Case 3**.

For **Case 1**, we write:

$$\begin{aligned} t_1\Lambda_3 &= t_1 2r \log \overline{u} - t_1 \log \overline{\alpha}^k - t_1 p \log \overline{\lambda} \\ &= t_1 2r \log \overline{u} - (q' t_2 - \delta p) \log \overline{\alpha}^k - t_1 p \log \overline{\lambda} \\ &= \log \left(\overline{u}^{t_1 2r} \overline{\alpha}^{-kq' t_2} \right) - p \log \left(\overline{\lambda}^{t_1} \overline{\alpha}^{-\delta k} \right). \end{aligned} \tag{4.33}$$

Then, we consider a linear form in two logarithms $\Lambda_2^1 = \log \beta_2 - p \log \beta_1$, where $\beta_1 = \overline{\lambda}^{t_1} \overline{\alpha}^{-\delta k}$ and $\beta_2 = \overline{u}^{t_1 2r} \overline{\alpha}^{-kq' t_2}$, and for this case we apply the proposition 4.3.2, following the explanation that we have presented after that proposition, but using now the Matveev's bounds for the linear form in three logarithms as an upper bound for p.

Let us turn now in to the **Case 2**. This time we write down

$$\begin{aligned} t_2\Lambda_3 &= t_2 2r \log \overline{u} - t_2 \log \overline{\alpha}^k - t_2 p \log \overline{\lambda} \\ &= q t_2 s_1' \log \overline{u} - t_2 \log \overline{\alpha}^k - t_2 p \log \overline{\lambda} \\ &= (t_1 + \delta p s_1') \log \overline{u} - t_2 \log \overline{\alpha}^k - t_2 p \log \overline{\lambda} \\ &= \log \left(\overline{\alpha}^{-kt_2} \overline{u}^{t_1 s_1'} \right) - p \log \left(\overline{u}^{-s_1} \overline{\lambda}^{t_2} \right). \end{aligned} \tag{4.34}$$

As before we turn out to have a linear form in two logarithms $\Lambda_2^2 = \log \gamma_2 - p \log \gamma_1$, where $\gamma_1 = \overline{u}^{-s_1} \overline{\lambda}^{t_2}$ and $\gamma_2 = \overline{\alpha}^{-kt_2} \overline{u}^{t_1 s_1'}$. We apply as before, the proposition 4.3.2 to this case, following also the same methods as before.

Table 4.8: Bounds for p using linear forms in three logarithms

D	p_0
17	40 902 094 178
33	157 752 030 294
41	35 994 070 812
57	429 407 772 757
63	69 516 630 329
65	49 434 815 608
68	16 382 452 021
73	808 303 621 445
90	29 188 841 666
97	2 552 797 449 913
98	8 383 577 486

Proposition 4.3.5. *Let D be one of the values in Table 4.5, with $c \neq 1$ and which the $p_0 \neq 10^3$. If D is in Table 4.4, the equation* (3.1) *does not have any solution for $p \geq p_0$, where p_0 is given in Table 4.8. If D is in Table 4.3 , the equation* (3.1) *does not have any non-trivial solution for $p \geq p_0$, where p_0 is given in Table 4.8, meaning, that the only solution is the trivial one, when $|y| = 1$.*

Proof. So we take $\alpha_1, \alpha_2, \alpha_3, b_1, b_2, b_3$ as in (4.27) and (4.28). We start by fixing $30 \leq r \leq 60$, $5 \leq L \leq 1500$, $1 \leq \chi \leq 30$ and $1 \leq m \leq 200$. We define $\rho := r/10$ and $\chi = c/10$. We define a_1, a_2, a_3 as in the Theorem 4.2. Then, we define $c_i, K, R_i, S_i, T_i, R, S$ and T as in the remarks above, with $i \in \{1, 2, 3\}$. We define b' as in the remark made above. After verying all the assumptions in the Theorem 4.2 we calculate a new bound p_1 using (4.29). Then we see if we verify ($\mathbf{C}_3$) and if we are **Case 1** or **Case 2**. If this is the case, then using the remarks above we compute new bounds p_2 associated to (4.30) and p_3 associated to one of the linear forms in two logs, (4.33) or (4.34). We finally take $p_0 = \max\{p_1, p_2, p_3\}$. **QED**

Table 4.9: Upper and lower bounds for p

D	c	p_{min}	p_{max}
2	1	13	4 111
3	1	13	7 793
5	1	13	1 759
8	1	13	4 111
10	1	13	13 291
15	1	13	16 433
17	1	13	16 843
	2	10^8	40 902 094 178
24	1	13	19 687
26	1	13	19 979
33	2	10^8	157 752 030 294
35	1	13	22 483
37	1	13	22 709
41	2	10^8	35 994 070 812
48	1	13	7 703
50	1	13	4 111
57	2	10^8	429 407 772 757
63	1	13	27 253
	3	10^8	69 516 630 329
65	1	13	27 367
	2	10^8	49 434 815 608
68	4	10^8	16 382 452 021
73	2	10^8	808 303 621 445
80	1	13	1 759
82	1	13	29 423
90	3	10^8	29 188 841 666
97	2	10^8	2 552 797 449 913
98	7	10^8	47 472 298 469
99	1	13	8 383 577 486

4.4 Proof of Theorem 1.1

We finally prove the main result of this thesis, Theorem 1.1. We will only look for the solutions of equation (**LN**), when n is a prime number p, since (**LN**) can be reduced to the equation (2.1) For $p = 2, 3, 5$ and D in our range, we use the methods presented in Chapter 2 to compute all the solutions for the equation (2.1). Recalling what we have seen in Chapter 3, we know that for the following values of $|D|$

$4, 6, 7, 11, 12, 13, 14, 18, 19, 23, 27, 28, 30, 31, 32, 34, 38, 39, 40, 42, 43, 44, 46, 47, 51, 53,$
$54, 56, 58, 59, 60, 61, 62, 66, 67, 69, 70, 71, 74, 76, 78, 79, 83, 86, 87, 88, 91, 92, 93, 95, 96,$

for $p \geq 7$ the equation (2.1) does not have any solution, except when $D = -4$, we only have the solution

$$(|x|, |y|, p) = \quad (2, 0, p).$$

Also in the same chapter we have proved that for $D = -22$, we only have the following solution

$$(|x|, |y|, p) = \quad (47, 3, 7),$$

and for $D = -94$, we also have, as the only solution of (2.1), the following:

$$(|x|, |y|, p) = \quad (421, 3, 11).$$

For the remaining values, we use the methods presented in this chapter. As we have proved above when $|D|$ is a square, that is, $D = -d^2$, for a integer number d, apart from the obvious solution $(|x|, |y|, p) = (d, 0, p)$, when $p \geq 7$, we only have another solution, when $D = -16$, the solution being

$$(|x|, |y|, p) = \quad (12, 2, 7).$$

When $|D| = 20, 21, 29, 45, 52, 55, 72, 75, 77, 84, 85$, Proposition 4.3.4 shows, that equation (2.1) does not have any solution for $p \geq 7$.

For the remaining values, using bounds provided by the linear forms in three logarithms, the method of Thue equations (Chapter 2) and the Kraus Methods (see Chapter 3), we have that, for $|D|$ in Table 4.9, if D is not a unit away from a square, then for $p \geq p_{max}$ and $7 \leq p \leq p_{min}$, the solutions of the equation 2.1 are given in Table A.1. When $p_{min} \leq p \leq p_{max}$, then we do not know if the equation (2.1), has a solution or not. For $D = 33, 41, 57, 68, 73, , 90, 97$ and 98 we could eliminate the case where the signature (d_1, d_2) associated to a solution (x, y, p) had $c = 1$ (see Lemma 4.3.1).

When $|D|$ is also in Table 4.9 and is a unit away from a square, then if $p \geq p_{max}$ and $7 \leq p \leq p_{min}$, the solutions of the equation 2.1 are given in Table A.1. Again, when $p_{min} \leq p \leq p_{max}$, then we do not know if the equation (2.1), does have another solution besides the obvious one, already mentioned in the Table A.1. Just notice that when D is a unit away from a square, and $c \neq 1$, using Kraus Methods, we were able to see that there were no solutions for $7 \leq p \leq 10^8$.

And this concludes the proof of Theorem 1.1.

4.5 What to do next?

As we have seen, there are some cases left to solve. If $D = 33, 41, 57, 68, 73.90, 97$ and 98 we are of the opinion that there are no solutions for equation (2.1) with $p \geq 7$. In chapter 5 we introduce a new Frey curve that might help us, to settle this once and for all, though, as we will explain in the mentioned chapter, we are not able to do so right now.

When D is a unit away from a square the equation has infinitely many solutions, and most available methods fail. There are techinques coming from Jacobians of curves (see for example [Sto98, Sto02, BMS$^+$08, BS08]), that can succeed for curves of small genus, which is not so in our case.

So when D is a unit away from a square the situation is still very obscure, though we are of the opinion that the only solutions to these cases, are the ones where $|y| = 1$, for all primes p.

Chapter 5

A new Frey curve

In this chapter we will study a new Frey curve associated to the exponent signature $(2, 3, p)$ of a ternary Diophantine equation. The aim of this study is to provide us a new Frey curve for the resolution of Diophantine equations via the modular approach. We begin by presenting the main result of this chapter

Theorem 5.1. *Let A, B, C, x, y, z be integers, such that $(Ax, By, Cz) = 1$. Let p be a prime number. Suppose also that for any prime number q we have*

(a) $v_q(A) \leq 1$;

(b) $v_q(B) \leq 2$;

(c) and $v_q(C) \leq p - 1$.

Finally we consider the equation

$$Ax^2 + By^3 = Cz^p. \tag{5.1}$$

The Frey curve associated to (5.1) *is*

$$E: \quad Y^2 = X^3 + 3AByX + 2A^2Bx. \tag{5.2}$$

Under the above assumptions we have:

(1) The minimal discriminant of E is

$$\Delta_{min} = \begin{cases} -2^6 3^3 A^3 B^2 C z^p & \text{if } v_2(Cz^n) < 6 \\ -2^{-6} 3^3 A^3 B^2 C z^p & \text{if } v_2(Cz^n) \geq 6 \end{cases}$$

(2) The conductor N of the curve E is given by

$$N := 2^{\epsilon_2} 3^{\epsilon_3} \operatorname{Rad}_{2,3}(AB)^2 \operatorname{Rad}_{2,3}(Cz),$$

where ϵ_3 is as given in Table 5.8 and ϵ_2 is as given in Table 5.7.

(3) Suppose that $p = 11$ or $p \geq 17$ and the curve E does not correspond to one of the equations:

$$11.(\pm 7)^2 - 1.(8)^3 = 3^3.(1)^{11}, \quad (\pm 43)^2 - 11^2.1^3 = 2^6.3^3.(1)^{11},$$
$$(\pm 4973)^2 - 11.(131)^3 = 2{\cdot}3^3.(1)^{11}, \quad 5.(\pm 14891)^2 - 17.373^3 = 2^6.3^3.2^{17},$$
$$5.(7717)^2 - 17^2(101)^3 = 2^7.3^3.(1)^{17}, \quad 19.3.(\pm 3)^2 - 1.(8.3)^3 = 1.(1)^{19},$$
$$5.(\pm 11.1433.11443)^2 - 7(137.2083)^3 = 2^6.3^3.(1)^{37}, \quad 5.(\pm 47)^2 - 7.11^3 = 2^6.3^3.(1)^{37},$$
$$3.43.(\pm 3^2.7) - 1.(2^4.5)^3 = (1)^{43}, \quad 3.67.(\pm 3.7.31)^2 - 1(2^3.5.11) = (1)^{67},$$
$$3.163.(\pm 3.7.11.19.127)^2 - 1.(2^4.5.23.29)^3 = (1)^{163}.$$

Then $E \sim_p f$ for some newform f of level

$$N_p = N := 2^{\epsilon_2} 3^{\epsilon} \operatorname{Rad}_{2,3}(AB)^2 \operatorname{Rad} 2, 3(C),$$

where ϵ_3 is as given in table 5.8 and ϵ_2 is as given in table 5.7 if $v_2(z) \neq 1$ or $p \neq 7$.

Proof. Both the discrimant Δ, and conductors N and N_p will be checked later on, in the following sections and looking at the Tables 5.7, 5.8, 5.9. About $E \sim_p f$ for some newform f of level N_p, we just use Theorem 3.3 item (1). After verifying

wich cases of our Diophantine equation of signature exponent $(2, 3, p)$ the cases mentioned in Table 3.1 correspond to, we exclude the equations mentioned in the statement of this theorem. And we have proved the Theorem. **QED**

5.1 Tate's Algorithm

Now we begin by recalling some facts and notation about elliptic curves (see for example [Coh07a, Chapter 7], [Sil85]). When we construct a Frey curve associated to a Diophantine equation, we are looking for the existence or not of a newform of a certain level. To know the level of the newforms we just need to know the conductor of the Frey curves, that is, the conductor of an elliptic curve. One way of doing it is to use Tate's algorithm, ([Tat75]) Before that, we need to recall some notation and results related to elliptic curves. Let

$$E : Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6, \tag{5.3}$$

an elliptic curve given in its Weierstrass equation, with $a_1, a_2, a_3, a_4, a_6 \in \mathbb{Q}$. We can simplify the equation by completing the square. Thus replacing Y by $\frac{1}{2}(Y - a_1X - a_3)$ gives an equation of the form

$$E : Y^2 = 4X^3 + b_2X^2 + 2b_4X + b_6,$$

where

$$b_2 = a_1^2 + 4a_2,\ b_4 = 2a_4 + a_1a_3, \text{and}\ \ b_6 = a_3^2 + 4a_6.$$

We also define quantities

$$b_8 = a_1^2 a_6 + 4a_2 a_6 - a_1 a_3 a_4 + a_2 a_3^2 - a_4^2,$$

$$c_4 = b_2^2 - 24 b_4,$$

$$c_6 = -b_2^3 + 36 b_2 b_4 - 216 b_6,$$

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

$$j_E = c_4^3 / \Delta.$$

One easily verifies that they satisfy the relations

$$4b_8 = b_2 b_6 - b_4^2 \text{ and } 1728\Delta = c_4^3 - c_6^2.$$

Further, if we replace (X, Y) by $((X - 3b_2)/36, Y/108)$, we eliminate the X^2 term, yielding the simpler equation

$$E : Y^2 = X^3 - 27 c_4 X - 54 c_6.$$

Two elliptic curves with different parameters may be isomorphic over $\mathbb{Q}$. Such an isomorphism must be given by the transformations $X = u^2 X' + r, Y = u^3 Y' + s u^2 X' + t$, where $r, s, t \in \mathbb{Q}, u \in \mathbb{Q}^*$. We obtain a new model for the same elliptic curve. Using the same quantities as those used in the formulas above, the parameters of the new model are given in Table 5.1

Now we introduce Tate's algorithm. We present the algorithm as it is given in [Coh00], Algorithms 7.5.1, 7.5.2 and 7.5.3, with some modifications provided by some facts that can be found in [Sil94, section IV.9]:

Algorithm 5.1.1 (Reduction of an Elliptic curve modulo a prime $p \geq 5$)**.** *Given integers a_1, a_2, a_3, a_4, a_6 and a prime $p > 3$, this algorithm determines the exponent f of p in the conductor of the elliptic curve*

$$E : \ Y^2 + a_1 XY + a_3 Y = X^3 + a_2 X^2 + a_4 X + a_6$$

Table 5.1: Formulas for the new model of a Elliptic curve

ua'_1	$=$	$a_1 + 2s$
$u^2a'_2$	$=$	$a_2 - sa_1 + 3r - s^2$
$u^3a'_3$	$=$	$a_3 + ra_1 + 2t$
$u^4a'_4$	$=$	$a_4 - sa_3 + 2ra_2 - (t + rs)a_1 + 3r^2 - 2st$
$u^6a'_6$	$=$	$a_6 + ra_4 + r^2a_2 + r^3 - ta_3 - t^2 - rta_1$
$u^2b'_2$	$=$	$b_2 + 12r$
$u^4b'_4$	$=$	$b_4 + rb_2 + 6r^2$
$u^6b'_6$	$=$	$b_6 + 2rb_4 + r^2b_2 + 4r^3$
$u^8b'_8$	$=$	$b_8 + 3rb_6 + 3r^2b_4 + r^3b_2 + 3r^4$
$u^4c'_4$	$=$	c_4
$u^6c'_6$	$=$	c_6
$u^{12}\Delta'$	$=$	Δ
j'	$=$	j

and integers u, r, s, t *such that* $a'_1, a'_2, a'_3, a'_4, a'_6$ *linked to* a_1, a_2, a_3, a_4, a_6 *via the formulas presented above give a model with the smallest possible power of* p *in its discriminant.*

1. *[Initialize] Compute* c_4, c_6, Δ *and* j*. If* $v_p(j) < 0$ *set* $k \leftarrow v_p(\Delta) + v_p(j)$ *else set* $k = v_p(\Delta)$*.*

2. *[Minimal?] If* $k < 12$ *set* $u \leftarrow 1, r \leftarrow 0, s \leftarrow 0$*, and* $t \leftarrow 0$*. Otherwise, set* $u \leftarrow p^{\lfloor k/12 \rfloor}$*; if* a_1 *is odd then set* $s \leftarrow (u - a_1)/2$ *else set* $s \leftarrow -a_1/2$*. Set* $a'_2 \leftarrow a_2 - sa_1 - s^2$*. Set* $r \leftarrow -a'_2, (u^2 - a'_2)/3$ *or* $(-u^2 - a'_2)/3$ *depending on* a'_2 *being congruent to 0, 1 or* -1 *modulo 3. Set* $a'_3 \leftarrow a_3 + ra_1$*. If* a'_3 *is odd, then set* $t \leftarrow (u^3 - a'_3)/2$ *else set* $t \leftarrow -a'_3/2$*. Finally, set* $k \leftarrow k \pmod{12}, \Delta \leftarrow \Delta/u^{12}, c_4 \leftarrow c_4/u^4$ *and* $c_6 \leftarrow c_6/u^6$*.*

3. *[Non-integral invariant] If* $v_p(j) < 0$*, then* k *must be equal to 0 or 6. If* $k = 0$*, set* $f \leftarrow 1$*. If* $k = 6$ *set* $f \leftarrow 2$*. Output* f, u, r, s, t *and terminate algorithm.*

4. *[Integral invariant] If* $k = 0$ *then set* $f \leftarrow 0$ *else set* $f \leftarrow 2$. *The possible values for* k *are* $0, 2, 3, 4, 6, 8, 9$ *and 10. Output* f, u, r, s, t *and terminate algorithm.*

For $p = 2$ or $p = 3$ the algorithm is much more complicated.

Algorithm 5.1.2 (Reduction of an Elliptic curve modulo 2 or 3). *Given integers* a_1, a_2, a_3, a_4, a_6 *and a prime* $p = 2$ *or 3, this algorithm determines the exponent* f *of* p *in the conductor of the elliptic curve*

$$E := Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6$$

and integers u, r, s, t *such that* $a'_1, a'_2, a'_3, a'_4, a'_6$ *linked to* a_1, a_2, a_3, a_4, a_6 *via the formulas presented above give a model with the smallest possible power of* p *in its discriminant. For* $i \in \{1, 2, 3, 4, 6\}$ *and* $k \in \mathbb{N}$ *we define* $a_{i,k} = a_i/p^k$.

1. *[Initialize] Set* $u \leftarrow 1, r \leftarrow 0, s \leftarrow 0,$ *and* $t \leftarrow 0$. *Compute* Δ *and* j *using the formulas given above. Set* $v \leftarrow v_p(\Delta)$.

2. *[Type* I_0*] If* $v = 0$ *then set* $f \leftarrow 0$ *and go to step 22.*

3. *[Type* I_v*] If* $p \nmid b_2 = a_1^2 + 4a_2$ *then set* $f \leftarrow 1$ *and go to step 22.*

4. *[Change equation] If* $p = 2$, *then set* $r_1 \leftarrow a_4 \pmod 2, s_1 \leftarrow (r_1 + a_2) \pmod 2$ *and* $t_1 \leftarrow (a_6 + r_1(a_4 + s_1)) \pmod 2$, *otherwise compute* b_6 *using the formulas above and set* $r_1 \leftarrow -b_6 \pmod 3, s_1 \leftarrow a_1 \pmod 3$ *and* $t_1 \leftarrow (a_3 + r_1a_1) \pmod 3$.

5. *[Type II] If* $p^2 \nmid a_6$, *then set* $f \leftarrow v$ *and go to step 22.*

6. *[Type III] Compute* b_8 *using the formulas above. If* $p^3 \nmid b_8$, *then set* $f \leftarrow v-1$ *and go to step 22.*

7. *[Type IV] Compute* b_6 *using the formulas above. If* $p^3 \nmid b_6$*, then set* $f \leftarrow v-2$ *and go to step 22.*

8. *[Change equation] If* $p^3 \nmid a_6$ *do the following. If* $p = 2$*, then set* $k \leftarrow 2$*, otherwise set* $k \leftarrow a_3 \pmod 9$*. Use formulas above with parameters* $1, 0, 0, k$ *to compute* $a'_1, \ldots, a'_6$*, then set* $a_1 \leftarrow a'_1, a_2 \leftarrow a'_2, \ldots, a_6 \leftarrow a'_6$ *and finally set* $t \leftarrow t + u^3 k$*.*

9. *[Type* I_0^**](At this point, we have* $p \mid a_2, p^2 \mid a_4$ *and* $p^3 \mid a_6$*.) Set* $P \leftarrow X^3 + a_{2,1}X^2 + a_{4,2}X + a_{6,3}$*. If* P *has distinct roots modulo* p*, then set* $f \leftarrow v - 4$ *and go to step 22.*

10. *[Change equation] Let* a *be the multiple root of the polynomial* P *modulo* p*. If* $a \neq 0$*, then use formulas above with parameters* $1, ap, 0, 0$ *to compute* $a'_1, \ldots, a'_6$*, then set* $a_1 \leftarrow a'_1, a_2 \leftarrow a'_2, \ldots, a_6 \leftarrow a'_6, r \leftarrow r + +u^2 ap$ *and* $t \leftarrow t + u^2 sap$*. If* a *is a double root go to step 16.*

11. *[Type* IV^**](Here* $p^2 \mid a_3, p^4 \mid a_6$*) Set* $P \leftarrow X^2 + a_{3,2}X + a_{6,4}$*. If* P *has a double root in* $\mathbb{F}_p$*, then let* a *be that root. Otherwise set* $f \leftarrow v - 6$ *and go to step 22.*

12. *[Change equation] If* $a \neq 0$ *the use once again the formulas above with parameters* $1, 0, 0, ap^2$ *to compute* $a'_1, \ldots a'_6$*. then set* $a_1 \leftarrow a'_1, \ldots, a_6 \leftarrow a'_6$ *and* $t \leftarrow t + u^3 ap^2$*.*

13. *[Type* III^**] If* $p^4 \nmid a_4$*, then set* $f \leftarrow v - 7$ *and go to step 22.*

14. *[Type* II^**] if* $p \nmid a_6$*, then set* $f \leftarrow v - 8$ *and go to step 22.*

15. *[Non-minimal equation] Using once again the formulas above with parameters* $p, 0, 0, 0$ *to compute* $a'_1, \ldots, a'_6$*, then set* $a_1 \leftarrow a'_1, \ldots, a_6 \leftarrow a'_6, u \leftarrow$

$pu, v \leftarrow v - 12$ *and go to step 2.*

16. *[Initialize loop]If* $p = 3$ *then set* $n = v - 6$. *For* $p = 2$ *set* $n = 0$. *Set* $v \leftarrow 1$ *and* $q \leftarrow p^2$. *Also set* $f \leftarrow v - 4 - n$, *so for* $p = 3$ *we have that* $f = 2$.

17. *[Type* I_v^*, *day in] Set* $P \leftarrow X^2 + a_{3,2+n/2}X - a_{6,4+n}$. *If* P *has distinct roots go to step 22, with* $n \leftarrow n + 1$ *if* $p = 2$.

18. *[Change equation] Let* a *be the double root of* P *modulo* p. *If* $a \neq 0$, *use formulas above with parameters* $1, 0, 0, aq$ *to compute* $a'_1, \ldots, a'_6$, *then set* $a_1 \leftarrow a'_1, \ldots, a_6 \leftarrow a'_6$ *and* $t \leftarrow t + u^3aq$.

19. *[Type* I_v^*, *day out] Set* $v \leftarrow v + 1$ *and* $P \leftarrow a_2/pX^2 + a_{4,3+n/2}X + a_{6,4+n}$. *If* P *has distinct roots modulo* p *go to step 22, with* $n \leftarrow n + 2$ *if* $p = 2$.

20. *[Change equation] Let* a *be the double root of* P *modulo* p. *If* $a \neq 0$ *use formulas above with parameters* $1, aq, 0, 0$ *to compute* $a'_1, \ldots a'_6$, *then set* $a_1 \leftarrow a'_1, \ldots, a_6 \leftarrow a'_6, r \leftarrow r + u^2aq$ *and* $t \leftarrow t + u^2saq$.

21. *[Loop] Set* $v \leftarrow v - 1$, $q \leftarrow p \times q, n \leftarrow n + 2$ *and go to step 17.*

22. *[Common termination] Output the numbers* f, u, r, s, t *and terminate the algorithm*

Let us turn now to the global counterpart of this process.

Algorithm 5.1.3 (Global reduction of an Elliptic curve). *Given integers* a_1, a_2, a_3,a_4, a_6, *this algorithm computes the arithmetic conductor* N *of the elliptic curve* $E := Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6$ *and integers* u, r, s, t *such that* $a'_1, a'_2, a'_3, a'_4, a'_6$ *linked to* a_1, a_2, a_3, a_4, a_6 *via the formulas presented above give a model with the smallest possible discriminant (in absolute value) and such that* $a'_1, a'_3 \in \{0, 1\}$ *and* $a'_2 \in \{0, \pm 1\}$.

1. *[Initialize] Set* $N \leftarrow 1, u \leftarrow 1, r \leftarrow 0, s \leftarrow 0$ *and* $t \leftarrow 0$. *Compute* $D \leftarrow |\Delta|$ *using formulas above.*

2. *[Finished] If* $D = 1$, *then output* N, u, r, s, t *and terminate algorithm.*

3. *[Local reduction] Find a prime divisor* p *of D. Then use Algorithm 5.1.2 or 5.1.1 to compute the quantities* f_p, u_p, r_p, s_p, t_p. *Set* $N \leftarrow Np^{f_p}$. *If* $u_p \neq 1$, *set* $u \leftarrow uu_p, r \leftarrow r + u^2 r_p, s \leftarrow s + us_p$ *and* $t \leftarrow t + u^3 t_p + u^2 s r_p$. *Finally set* $D \leftarrow D/p^{v_p(D)}$. *Go to step 2.*

5.1.1 Papadopoulos' tables for the exponent of the conductor of an elliptic curve

It is possible to compute the conductor of an elliptic curve using instead the information provided in the paper by I. Papadopoulos [Pap93], which provides all possible cases for the value of the exponent of a given prime in the conductor of an elliptic curve. This information is set in tables, that I will reproduce here (Tables 5.4,5.3,5.2) and we will use it to estimate possible values for the exponent for a given prime of the conductor and for the valuation of Δ for that same prime.

As before, let E be an elliptic curve over $\mathbb{Q}$, as in (5.3), with a_1, a_2, a_3, a_4, a_6 rational integers. Let c_4, c_6 and Δ be as before and let N be the conductor for the elliptic curve. In his paper, Papadopoulos presents us tables with the results for $v_p(N)$ for a given prime p (distinguishing the cases $p = 2$, $p = 3$ and $p \geq 5$), according to the valuations $v_p(c_4), v_p(c_6), v_p(\Delta)$, to Néron types, Tate's cases and Kodaira symbols.

As we can see in Tables 5.3 and 5.4 we might have cases where though we have the same $(v_p(c_4), v_p(c_6), v_p(\Delta))$ we might end up with different values of f_p. Now we show how to distinguish each case, following Papadopoulos' paper. We

start for $p = 3$. In his paper, Papadopoulos uses the following terminology: we say that a curve satisfies property P_i if there exists $x \in \mathbb{Z}$ such that $x^3 - 3c_4x - 2c_6 \equiv \pmod{3^{3+i}}$. For $i = 2, 5$ we have that the condition P_i in the table is equivalent to the condition: there exists $y \in \mathbb{Z}$ such that

$$y^3 + b_2y^2 + 8b_4y + 16b_6 \equiv 0 \pmod{3^i}.$$

For $p = 2$ the situation is a bit more messy. We have the following proposition.

Proposition 5.1.1. *Let E be an elliptic curve with Weierstrass form 5.3 that corresponds in Table 5.4 to a Tate's case ≥ 3. There exist $r, t \in \mathbb{Z}$ such that*

$$2 \mid a_4 + r^2, \quad 2 \mid t^2 + a_4a_2 - a_6.$$

We define

$$a_2(r, s) := a_2 + 3r - sa_1 - s^2,$$
$$a_6(r, t) := a_6 + ra_4 + r^2a_2 + r^3 - ta_3 - t^2 - rta_1,$$
$$b_6(r, x) := b_6 + 2rb_4 + r^2b_2 + 4r^3 - x^2,$$
$$b_8(r) := b_8 + 3rb_6 + 3r^2b_4 + r^3b_2 + 3r^4.$$

1) *If $a_6(r, t) \equiv 0 \pmod 4$ then we are in a case ≥ 4.*

2) *If $b_8(r) \equiv 0 \pmod 8$ then we are in a case ≥ 5.*

3) *If $b_8(r) not \equiv 0 \pmod{2^5}$ we are in Tate's case 6, type I_0^*.*

4) *If $b_8(r) \equiv 0 \pmod{2^5}$, then there exists $t \in \mathbb{Z}$ such that $a_6(r, t) \equiv 0 \pmod 8$. Choose such a t. We are in case 6 if we have $v_2(a_6(r, t)) = 3$), otherwise we are in a case ≥ 7.*

5) *If* $b_8(r) \equiv 0 \pmod{2^5}$ *and there exists* $s \in \mathbb{Z}$ *such that* $a_2(r,s) \equiv 0 \pmod{4}$, *then we are in a case* ≥ 8.

6) *If* $v_2(b_8(r)) \geq 7$ *we are in case* ≥ 10.

7) *If* $v_2(c_4) \geq 8$ *and* $v_2(\Delta) \leq 12$. *Exists* $r \in \mathbb{Z}$ *such that* $v_2(b_8(r)) \geq 8$. E *is a non-minimal equation if exist* $x \in Z$ *such that*

$$v_2(b_6(r,x)) \geq 8,$$

otherwise we are in case 10.

8) *If* $v_2(c_4) \leq 4$, *then exists* $r \in \mathbb{Z}$ *such that* $v_2(b_8(r)) \geq 8$ *and a* $t \in \mathbb{Z}$ *such that*

$$v_2(a_6(r,t)) \geq 5.$$

If $v_2(a_6(r,t)) \geq 6$, *then* E *is non-minimal.*

5.2 The Frey curve associated to the Diophantine equation with signature $(2,3,n)$

As we have said before we interested in providing a recipe for solving the ternary Diophantine equation of signature $(2,3,p)$ (5.1). But we will study a more general case. Consider the equation

$$Ax^2 + By^3 = Cz^n, \tag{5.4}$$

where $n \in \mathbb{N}$ is greater than or equal to 2, $A, B, C, x, y, z \in \mathbb{Z} \setminus \{0\}$, such that

1) $(Ax, By, Cz) = 1$;

2) and $\forall p$ prime we have:

Table 5.2: Papadopoulos' table for $p \geq 5$

Kodaira symbol	I_0		$I_{t,(t>0)}$	II	III	IV	I_0^*		$I^*_{t,(t>0)}$	IV^*	III^*	II^*	Non minimal equation
Néron's type	A		B_t	C_1	C_2	C_3	C_4		$C_{5,t}$	C_6	C_7	C_8	
Tate's case	1		2	3	4	5	6		7	8	9	10	
$v_p(c_4)$	0	≥ 0	0	≥ 1	1	≥ 2	2	≥ 2	2	≥ 3	3	≥ 4	≥ 4
$v_p(c_6)$	≥ 0	0	0	1	≥ 2	2	≥ 3	3	3	4	≥ 5	5	≥ 6
$v_p(\Delta)$	0	0	t	2	3	4	6	6	$6+t$	8	9	10	≥ 12
$v_p(N)$	0	0	1	2	2	2	2	2	2	2	2	2	

Table 5.3: Papadopoulos' table for $p = 3$

Kodaira symbol	I_0		$I_{t,(t>0)}$	II				III		IV			I_0^*	$I^*_{t,(t>0)}$	IV^*				III^*		II^*			Non minimal equation		
Néron's type	A		B_t	C_1				C_2		C_3			C_4	$C_{5,t}$	C_6				C_7		C_8					
Tate's case	1		2	3				4		5			6	7	8				9		10					
$v_3(c_4)$	0	1	0	≥ 2	2	2	≥ 3	≥ 2	2	2	3	≥ 4	2	3	2	≥ 4	4	4	≥ 5	≥ 4	4	4	5	≥ 6	4	5	≥ 6
$v_3(c_6)$	0	≥ 3	0	3	4	3	4	3	≥ 5	3	5	5	3	≥ 6	3	6	7	6	7	6	≥ 8	6	8	8	6	≥ 9	≥ 9
$v_3(\Delta)$	0	0	t	3	3	4	5	3	3	5	6	7	6	6	$6+t$	9	9	10	11	9	9	11	12	13	≥ 12	12	≥ 15
Extra Conditions				not P_2				P_2								not P_5				P_5							
$v_3(N)$	0	0	1	3	3	4	5	2	2	3	4	5	2	2	2	3	3	4	5	2	2	3	4	5			

Table 5.4: Papadopoulos' table for $p = 2$

Kodaira symbol	I_0		$I_{t,(t>0)}$	II				III					IV		I_0^*			
Néron's type	A		B_t	C_1				C_2					C_3		C_4			
Tate's case	1		2	3				4					5		6			
$v_2(c_4)$	0	≥ 4	0	≥ 4	4	4	≥ 5	4	5	4	5	5	4	≥ 6	4	4	≥ 6	≥ 6
$v_2(c_6)$	0	3	0	5	≥ 6	6	6	5	5	≥ 6	7	≥ 8	5	5	6	6	7	8
$v_2(\Delta)$	0	0	t	4	6	7	6	4	4	6	8	9	4	4	8	9	8	10
Extra Conditions				$(*)$	$(*)$			$(*)$	$(*)$	$(*)$			$(*)$	$(*)$	$(*)$		$(*)$	
$v_2(N)$	0	0	1	4	6	7	6	3	3	5	7	8	2	2	4	5	4	6

Kodaira symbol	I_1^*		I_2^*			I_3^*		$I_{t,t\geq 4}^*$		IV^*		III^*				II^*			Non minimal equation		
Néron's type	$C_{5,1}$		$C_{5,2}$			$C_{5,3}$		$C_{5,t}$		C_6		C_7				C_7					
Tate's case	7									8		9				10					
$v_2(c_4)$	4	6	4	6	6	4	6	4	6	4	≥ 7	4	7	7	7	4	≥ 8	≥ 8	4	≥ 8	≥ 8
$v_2(c_6)$	6	7	6	≥ 9	9	6	≥ 9	6	9	6	7	6	9	10	≥ 11	6	9	10	6	9	≥ 11
$v_2(\Delta)$	8	8	10	12	13	11	12	$8+t$	$10+t$	8	8	10	12	14	15	11	12	14	≥ 12	12	≥ 16
Extra Conditions	$(*)$	$(*)$	$(*)$	$(*)$		$(*)$	$(*)$	$(*)$		$(*)$	$(*)$	$(*)$				$(*)$	$(*)$		$(*)$	$(*)$	
$v_2(N)$	3	3	4	6	7	4	5	4	6	2	2	3	5	7	8	3	4	6			

Table 5.5: Coefficients and quantities for the Frey curve $E_{(2,3,n)}$

a_1	$=$	0
a_2	$=$	0
a_3	$=$	0
a_4	$=$	$3ABy$
a_6	$=$	$2A^2Bx$
b_2	$=$	0
b_4	$=$	$6ABy$
b_6	$=$	$8A^2Bx$
b_8	$=$	$-9A^2B^2y^2$
c_4	$=$	$-2^4 3^2 ABy$
c_6	$=$	$-2^6 3^2 A^2 Bx$
Δ	$=$	$-2^6 3^3 A^3 B^2 (Ax^2 + By^3) = -2^6 3^3 A^3 B^2 Cz^n$
$j_{E_{(2,3,n)}}$	$=$	$2^6 3^3 By^3 / Cz^n$

2.1) $v_p(A) \leq 1$;

2.2) $v_p(B) \leq 2$;

2.3) $v_p(C) \leq n - 1$.

Consider now the Frey curve attached to equation (5.4)

$$E_{(2,3,n)} : \quad Y^2 = X^3 + 3AByX + 2A^2Bx, \tag{5.5}$$

similar to the Frey curve (5.2). Following the notation above, we have coefficients and quantities mentioned above, relatively to our Frey curve (5.5), summarized in Table 5.5.

5.2.1 The conductor of our Frey curve $E_{(2,3,n)}$

We start applying the algorithm 5.1.3. First we have that

$$D := |\Delta| = 2^6 3^3 A^3 B^2 (Ax^2 + By^3) = 2^6 3^3 A^3 B^2 Cz^n.$$

Let p be a prime. Since $D \neq 1$, we will consider three cases first when $p = 2$, then $p = 3$ and finally $p \geq 5$.

5.2.2 Exponent for $p = 2$.

We start by applying algorithm 5.1.2 for $p = 2$. We start by setting $u \leftarrow 1, r \leftarrow 0, s \leftarrow 0, t \leftarrow 0$,

$$v = v_2(\Delta) = \begin{cases} 6 + 3v_2(A) & \text{if } 2 \mid Ax, \\ 6 + 2v_2(B) & \text{if } 2 \mid By, \\ 6 + v_2(C) + nv_2(z) & \text{if } 2 \mid Cz. \end{cases} \tag{5.6}$$

If $v = 0$ then $f_2 = 0$ and we have finished, but from (5.6) we see that $v \geq 6$, so we proceed to the next step of the algorithm 5.1.2. In step 3, if $p \nmid b_2$, we have that $f_2 = 1$ and we have finished, but we have that $b_2 = 0$, so we proceed to the next step of the algorithm. We set

$$r_1 \equiv a_4 \pmod 2,$$
$$s_1 \equiv r_1 + a_2 \pmod 2, \text{ and}$$
$$t_1 \equiv a_6 + r_1(a_4 + s_1) \pmod 2.$$

With these parameters and $u = 1$, using the formulas given in Table 5.1 we calculate the new coefficients $a'_1, \ldots, a'_6$. From the definition of r_1, s_1, t_1 and from Table 5.5 we have that

$$s_1 \equiv r_1 + a_2 \equiv a_4 + a_2 \equiv a_4 \pmod 2,$$
$$t_1 = a_6 + r_1(a_4 + s_1) \equiv a_6 + r_1(r_1 + r_1) \equiv a_6 \equiv 0 \pmod 2.$$

Therefore we see that r_1 and s_1 depend on $a_4 \pmod 2$, and t_1 is always 0. Now we have that $a_4 = 3ABy$, that means that $a_4 \equiv ABy \pmod 2$. Suppose that

we have $2 \mid ABy$, therefore $a_4 \equiv 0 \pmod 2$. Now $2 \mid ABy$ is equivalent to have $v_2(A) = 1$ or $v_2(B) \geq 1$ or $v_2(y) \geq 1$. We will separate this in three cases:

I $v_2(A) = 1$, which implies that $a_4 \equiv 0 \pmod 2$, so $r_1 = s_1 = 0$. In this case we have that $v_2(c_4) = 5, v_2(c_6) \geq 8$ and $v = 9$.

II $v_2(B) \geq 1$, so $a_4 \equiv 0 \pmod 2$, which implies that $r = s = 0$. For this case we have that $v_2(c_4) \geq 5, v_2(c_6) \in \{7, 8\}$ and $v \in \{8, 10\}$.

III $v_2(B) = 0$ and $v_2(y) \geq 1$, once again $a_4 \equiv 0 \pmod 2$ and $r = s = 0$. When it comes to the 2-valuation of c_4, c_6 and Δ we have that, $v_2(c_4) \geq 5, v_2(c_6) = v = 6$, since we assume in this case that $v_2(B) = 0$.

We must not forget the other case

IV $v_2(ABy) = 0$. In this case $a_4 \equiv 1 \pmod 2$, so we have this time that $r = s = 1$. We also have that $v_2(c_4) = 4, v_2(c_6) \geq 6$ and $v \geq 6$.

Let us start with case **I**. Take $v_2(A) = 1$. Therefore $a_4 \equiv 0 \pmod 2$, thus we have $r_1 = s_1 = 0$ and $t_1 = 0$. Using $u = 1, r = 0, s = 0, t = 0$ and the formulas from Table 5.1 we keep the same values of $a_1, a_2, a_3, a_4, a_6, b_2, b_4, b_6$ and b_8. We have also the following quantities:

$$v_2(c_4) = 5, \quad v_2(c_6) \geq 8 \quad \text{and} \quad v = 9.$$

According to Papadopoulos' tables, we are in the Tate's case 4, and we expect to have $f_2 = 8$. We move to the next step. So in step 5, if $p^2 \nmid a_6$ we set $f_2 = v$ and finish. We have that $a_6 = 2A^2Bx$, so we have that $v_2(a_6) \geq 3$. Therefore we proceed to the next step. In step 6, if $p^3 \nmid b_8$ then set $f_2 = v - 1$ and finish. Now $b_8 = -9A^2B^2y^2$, and we have that $v_2(b_8) = 2$, so $8 \nmid b_8$. So if $v_2(A) = 1$, then $f_2 = v - 1 = 8$, as expected. Now we move to case **II**. Now we have $v_2(B) \geq 1$

and simple calculation show us we have $a_1, \ldots, a_6, b_2, \ldots, b_8$ as in case **I**. For this case we have that:

$$v_2(c_4) \geq 5, \quad v_2(c_6) \in \{7, 8\} \quad \text{and} \quad v \in \{8, 10\}.$$

We now move to step 5. If $p^2 \nmid a_6$ then we set $f_2 = v$ and we are finished. As before $a_6 = 2A^2Bx, v_2(a_6) = 1 + v_2(B) \geq 2$, so $4 \mid a_6$. We proceed to step 6. If $p^3 \nmid b_8$ then set $f = v - 1$ and finish. We have that $b_8 = 9A^2B^2y^2$ so $v_2(b_8) = 2v_2(B) + 2v_2(y)$. If $v_2(B) = 1$ then we have $v_2(b_8) = 2 + 2v_2(y)$. So we have then

II.1 if $v_2(y) = 0$, then $8 \nmid b_8$. For this case we have that $v_2(c_4) = 5, v_2(c_6) = 7$ and $v = 8$.

II.2 if $v_2(y) \geq 1$, then $8 \mid b_8$. In this case we have that $v_2(c_4) \geq 5, v_2(c_6) = 7$ and $v = 8$.

We also have a third case, **II.3**, $v_2(B) = 2$. It is clear to see that $8 \mid b_8$, and also that

$$v_2(c_4) \geq 6, \quad v_2(c_6) \geq 8 \quad \text{and} \quad v = 10.$$

If we are in case **II.1**, that is, $v_2(B) = 1$ and $v_2(y) = 0$ then we have $f_2 = v - 1 = 7$, that corresponds to the Tate's case 4 in Papadopoulos' table. For cases **II.2** and **II.3** we proceed to the next step. We are now in Step 7. If $p^3 \nmid b_6$ then $f_2 = v - 2$ and we have finished. We have that $b_6 = 8A^2Bx$, and so $v_2(b_6) \geq 4$, so $8 \mid b_6$. We proceed to step 8. Does $p^3 \mid a_6$? We have that $a_6 = 2A^2Bx$. From the case **II.2** we see that $v_2(a_6) = 2$ while from the case **II.3** we see that $v_2(a_6) = 3$. So now treat each case separately. First case we consider is **II.2**. Since we have $v_2(a_6) = v_2(2A^2Bx) = 1 + v_2(B) = 2$, following the procedures of the algorithm

we use $u = 1, r = 0, s = 0, t = 2$ to compute $a_1, \ldots, a_6$, using the formulas in Table 5.1. Therefore we have:

$$a'_1 = 0, \quad a'_2 = 0, \quad a'_3 = 4,$$
$$a'_4 = 3ABy, \quad a'_6 = 2A^2Bx - 4.$$

Now we move to the next step. So now we have that $2 \mid a_2 = 0$, $2^2 \mid a_4 = 3ABy$, true since $v_2(By) \geq 2$ and finally $2^3 \mid a_6 = 2A^2Bx - 4$. Since $v_2(B) = 1$ and A is odd, we have that $a_6 \equiv 0 \pmod 8$. Set $P = X^3 + a_{2,1}X^2 + a_{4,2}X + a_{6,3}$. It is easy to see that $a_4 \equiv 0 \pmod 8$ if and only if $v_2(y) \geq 2$. Now let us take a look at the equality $a_6 \equiv 0 \pmod{16}$, that is equivalent to see that $2A^2Bx - 4 \equiv 0 \pmod{16}$. We have $2A^2Bx - 4 \equiv 0 \pmod{16}$ if and only if $2A^2Bx \equiv 4 \pmod{16}$. $v_2(2A^2Bx) = 2$, we have that or either $2Bx \equiv 4$ or $12 \pmod{16}$. So from what we have seen, we have that $a_{4,2} \equiv 1 \pmod 2$ if and only if $v_2(y) = 1$ otherwise we have $a_{4,2} = 0 \pmod 2$, and $a_{6,3} \equiv 0 \pmod 2$ if and only if $2A^2Bx \equiv 4 \pmod{16}$, and $a_{6,3} \equiv 1 \pmod 2$ if and only if $2A^2Bx \equiv 12 \pmod{16}$. So we have four cases:

II.2.1 $v_2(y) \geq 2$ and $2A^2Bx \equiv 4 \pmod{16}$, where $v_2(c_4) = 6, v_2(c_6) = 7$ and $v = 8$. So by Papadopoulos $f_2 = 4$ (resp. 3) in Tate's case 6^* (resp. 7^*). And we also have that $P \equiv X^3 + X \equiv X(X^2 + 1) = X(X + 1)^2 \pmod 2$, which has a multiple root, $a = 1$ of multiplicity 2 in $\overline{\mathbb{F}_p}$.

II.2.2 $v_2(y) \geq 2$ and $2A^2Bx \equiv 12 \pmod{16}$. For this case we have that $v_2(c_4) = 6, v_2(c_6) = 7$ and $v = 8$, by what we have seen before of Papadopoulos' table, we are expecting f_2 to be equal to 4 (resp 3), when we are in Tate's case 6^* (resp. 7^*). Our polynomial is of the form $P \equiv X^3 + X + 1 \pmod 2$ which has simple roots in $\overline{\mathbb{F}_p}$.

II.2.3 $v_2(y) = 1$ and $2A^2Bx \equiv 4 \pmod{16}$. Therefore we have that $v_2(c_4) \geq 7, v_2(c_6) = 7$ and $v = 8$. So accordingly to Papadopoulos' we expect that $f_2 = 4$ (resp. 2) in the Tate's case 6^* (resp. 8^*). Our polynomial turns out to be of the form $P \equiv X^3 \pmod{2}$, which has a multiple root $a = 0$ of multiplicity 3 over $\overline{\mathbb{F}_p}$.

II.2.4 $v_2(y) = 1$ and $2A^2Bx \equiv 12 \pmod{16}$. For this case we see that we have $v_2(c_4) \geq 7, v_2(c_6) = 7$ and $v = 8$. As in the previous case we can expect that f_2 will be equal to 4 (resp. 2) when we are in Tate's case 6^* (resp. 8^*). On the other hand, our polynomial turns out to be $P \equiv X^3 + 1 = (X+1)(X^2+X+1)$ which has simple roots over $\overline{\mathbb{F}_p}$.

We start with the case **II.2.1** At this point we have

$$v_2(y) = v_2(B) = 1, \quad 2A^2Bx \equiv 4 \pmod{16},$$
$$v_2(c_4) = 6, \quad v_2(c_6) = 7, \quad v = 8, \text{ and }, \quad P \equiv X(X+1)^2 \pmod{2}.$$

We have that P has a root $a = 1$ of multiplicity 2. We move on to step 10 Using $a = 1$, and $u_1 = 1, r_1 = 2a, s_1 = t_1 = 0$ we compute new coefficients a_1, a_2, a_3, a_4, a_6. ($u = 1, r = 2, s = 0, t = 2$ for output).

$$a_1' = 0, \quad a_2' = 6, \quad a_3' = 4,$$
$$a_4' = 3ABy + 12, \quad a_6' = 2A^2Bx + 6ABy + 4.$$

Since a is a double root we move to step 16. In step 16 we set $n = 0$ and $f_2 = v - 5 - n$. Now we proceed to the next step. For step 17 set $P = X^2 + a_{3,2}X - a_{6,4} \equiv X^2 + X + a_{6,4} \pmod{2}$, since $a_{3,2} = 1$. And therefore either $P \equiv X^2 + X = X(X+1) \pmod{2}$ or $P = X^2 + X + 1 \pmod{2}$, and both of these polynomials have simple roots in $\overline{\mathbb{F}_p}$, so $f_2 = v - 5 = 3$, which by

Papadopoulos' table we are in Tate's case 7^*. To see that we are in Tate's case 7^*, we need to find $r \in \mathbb{Z}$ such that $v_2(b_8(r)) \geq 5$ and given that r that there isn't $s \in \mathbb{Z}$ such that $a_2(r,s) \equiv 0 \pmod 4$. We see that $v_2(b_8(r)) \geq 5$ implies that $r \equiv 2 \pmod 4$, and therefore we have that $a_2(r,s) \equiv 0 \pmod 4$ is equivalent to have $s^2 \equiv 2 \pmod 4$, which is impossible, so we are in case Tate 4.

We turn our attention to the case **II.2.2**. In this case we have

$$v_2(y) = v_2(B) = 1, \quad 2A^2Bx \equiv 12 \pmod{16},$$
$$v_2(c_4) = 6, \quad v_2(c_6) = 7, \quad v = 8, \text{ and}$$
$$P \equiv X^3 + X + 1 \pmod 2.$$

As we have seen before, we have that P has simple roots over $\overline{\mathbb{F}_p}$ and so $f_2 = v - 4 = 4$, case Tate 6^*, according to Papadopoulos. To prove that we are in case Tate 6^* we need to see if the congruence $v_2(b_8(r)) \geq 5$ does have a solution for an $r \in \mathbb{Z}$. If not then we are in case 6^*. If it has a solution, then there exists $t \in \mathbb{Z}$ such that $v_2(a_6(r,t)) \geq 3$. We are in case 6^* if we have $v_2(a_6(r,t)) = 3$. It's easy to see that $r \equiv 2 \pmod 4$, we have that $v_2(b_8(r)) \geq 5$, and that's the only case when we have this congruence. Now picking up $t = 2$ we have that $a_6(r,t) \equiv 8 \pmod{16}$, that is $v_2(a_6(r,t)) = 3$. So we are in case Tate 6^*.

We consider this time the case **II.2.3**. Remember that in this case we have

$$v_2(y) \geq 2, \quad v_2(B) = 1, \quad 2A^2Bx \equiv 4 \pmod{16},$$
$$v_2(c_4) \geq 7, \quad v_2(c_6) = 7, \quad v = 8, \text{ and} \quad P \equiv X^3 \pmod 2.$$

So P has a multiple root in $a = 0$ of multiplicity 3 over $\overline{\mathbb{F}_p}$. Since $a = 0$ and has multiplicity 3 we move to step 11. In this step we have that $p^2 \mid a_3 = 4$ and $p^4 \nmid a_6 = 2A^2Bx - 4$. Set $P = X^2 + a_{3,2}X + a_{6,4} \equiv X^2 + X + a_{6,4}$. So as in case **II.2.1** step 17, we have that P will have simple roots over $\overline{\mathbb{F}_p}$. Therefore

$f_2 = v - 6 = 2$, which is case Tate 8^* accordingly to Papadopoulos' table. To prove this, since we only need to distinguish between case 6^* and case 8^*, we first see if there is and $r \in \mathbb{Z}$ such that $v_2(b_8(r)) \geq 5$ and if so, show that all $t \in \mathbb{Z}$ such that $v_2(a_6(r,t)) \geq 3$ imply that $v_2(a_6(r,t)) > 3$. First we use `MAGMA` to see that $v_2(b_8(r)) \geq 5$ implies that $r \equiv 0 \pmod 4$, and then that when there is a $t \in \mathbb{Z}$ such that $v_2(a_6(r,t)) \geq 3$ we have that $t \equiv 2 \pmod 4$ and $v_2(a_6(r,t))$ is always greater than 3. And we are done with this case.

Now we finally consider the case **II.2.4**. As before, recall that we have

$$v_2(y) \geq 2, \quad v_2(B) = 1, \quad 2A^2Bx \equiv 12 \pmod{16},$$
$$v_2(c_4) \geq 7, \quad v_2(c_6) = 7, \quad v = 8, \text{ and } \quad P \equiv X^3 + 1 \pmod 2.$$

Since P has simple roots over $\overline{\mathbb{F}_p}$, we have that $f_2 = v - 4 = 4$, so we are in case Tate 6^*. As before, we need to see if there is an $r \in \mathbb{Z}$ such that $v_2(b_8(r)) \geq 5$, then for that r there is an $t \in \mathbb{Z}$ such that $v_2(a_6(r,t)) = 3$. For $r \equiv 0 \pmod 4$ we have that $b_8(r) \equiv 0 \pmod{32}$ and that when there is a $t \in \mathbb{Z}$ such that $v_2(a_6(r,t)) \geq 3$, we have that $a_6(r,t) \equiv 8 \pmod{16}$. So this proves we are in case 6^*.

Now we go back to the case **II.3**. In this case we have $v_2(B) = 2$. Looking at c_4, c_6 and Δ we have the following congruences:

$$v_2(c_4) \geq 6, \quad v_2(c_6) = 8, \quad v = 10,$$

and we have that $a_6 \equiv 0 \pmod 8$. So we move on to the next step. We are now in step 9 and we have that $p \mid a_2 = 0$, $p^2 \mid a_4 = 3ABy$ and $p^3 \mid a_6 = 2A^2Bx$. Set $P = X^3 + a_{2,1}X^2 + a_{4,2}X + a_{6,3}$. Now we have that $a_{6,3} \equiv 1 \pmod 2$ and $a_{2,1} = 0$. Our choices for P are $P = X^3 + X + 1$ or $P = X^3 + 1 = (X+1)(X^2 + X + 1)$ which in both cases have simple roots over $\overline{\mathbb{F}_p}$, therefore $f_2 = v - 4 = 6$, which is case Tate 6, by Papadopoulos' table.

We move on to case **III**, where we have $v_2(y) \geq 1$ and $v_2(B) = 0$. In this case we have that $v_2(c_4) \geq 5, v_2(c_6) = 6$ and $v = 6$. By Papadopoulos' table we are in case Tate 3 and are expecting f_2 to be equal to 3. In step 5 we have that if $p^2 \nmid a_6$, then $f_2 = v$ and we have finished. Recall that at this point we have $a_6 = 2A^2Bx$ and so $v_2(a_6) = 1$. Therefore $4 \nmid a_6$ and we have $f_2 = v = 3$, as it was predicted.

Now we turn to case **IV**, where we assume that $v_2(A) = v_2(B) = v_2(y) = 0$, that is, ABy is odd, therefore we have $r_1 = s_1 = 1$.

Then we turn to step 4. From what we have seen above we have $r_1 = s_1 = 1$ and $t_1 = 0$. As consequence, we now use the parameters $u = r = s = 1$ and $t = 0$ as the Formulas of the Table 5.1, and we have new coefficients, that are:

$$a_1' = 2, \quad a_2' = 2, \quad a_3' = 0,$$
$$a_4' = 3ABy + 3, \quad a_6' = 2A^2Bx + 3ABy + 1$$

We move now to the next step. In step 5 if $p^2 \nmid a_6$ then we have $f_2 = v$, and as before, we have finished. Now $a_6 = 2A^2Bx + 3ABy + 1$, so $a_6 \equiv 0 \pmod 4$ if and only if $2A^2Bx + 3ABy + 1 \equiv 0 \pmod 4$ If we have $v_2(x) \geq 1$ then the equality above turns to be $3ABy \equiv 3 \pmod 4$. When $v_2(x) = 0$, then $a_6 \equiv 0 \pmod 4$ if and only if $3ABy \equiv 1 \pmod 4$. So we have the following cases:

IV.1 $v_2(x) = 0$ and $ABy \equiv 1 \pmod 4$, where $p^2 \nmid a_6$.

IV.2 $v_2(x) = 0$ and $ABy \equiv 3 \pmod 4$, where $p^2 \mid a_6$.

IV.3 $v_2(x) \geq 1$ and $ABy \equiv 1 \pmod 4$, where $p^2 \mid a_6$.

IV.4 $v_2(x) \geq 1$ and $ABy \equiv 3 \pmod 4$, where $p^2 \nmid a_6$.

We study each case separately from now on, starting with case **IV.1**

So we have that

$$v_2(x) = 0 \quad ABy \equiv 1 \pmod 4$$
$$v_2(c_4) = 4, \quad v_2(c_6) = 6, \text{ and } \quad v \geq 7,$$

since $AxBy$ is an odd number so Cz must be even. We also have that $p^2 \nmid a_6$ so $f_2 = v$, and looking at the table above, we see that the only case with $v_2(c_4) = 4, v_2(c_6) = 6, v \geq 7$ and $f_2 = v$ is the case Tate 3, with $v = 7$. In fact using MAGMA we can show that in this case we could only have $v_2(Cz^n) = 1$, we just need to consider all possible $A, x, B, y \pmod 4$ that satisfy the assumptions above and see that $Ax^2 + By^2 \equiv 2 \pmod 4$.

We move on to case **IV.2**, where we have that

$$v_2(x) = 0 \quad ABy \equiv 3 \pmod 4$$
$$v_2(c_4) = 4, \quad v_2(c_6) = 6, \text{ and } \quad v \geq 7.$$

As we have seen before we have that $p^2 \mid a_6$ and $v_2(Cz^n) \geq 1$. In fact we can prove that $v_2(Cz^n) \geq 2$. Since $Ax^2+By^3 \equiv Cz^n \pmod 4$, we have that $A+By \equiv Cz^n \pmod 4$, since $ABxy$ is odd. By the same reason we have that $1+ABy \equiv ACz^n \pmod 4$, since $ABy \equiv 3 \pmod 4$ and A is odd then $4 \mid Cz^n$. Now we move on to step 6, since $p^2 \mid a_6$. If $p^3 \nmid b_8$ then set $f_2 = v - 1$ and we have finished. Now $b_8 = b_8 + 3rb_6 + 3r^3b_4 + r^3b_2 + 3r^4 = -9A^2B^2y^2 + 24A^2Bx + 18ABy + 13$, so $b_8 \equiv 0 \pmod 8$ if and only if $2ABy \equiv 6 \pmod 8$, which is true, so we move on to step 7 If $p^3 \nmid b_6$ then $f_2 = v - 2$ and we have finished. We have that $b_6 = b_6 + 2rb_4 + r^2b_2 + 4r^3 = 8A^2Bx + 12ABy + 4$. So $b_6 \equiv 0 \pmod 8$ if and only if $3ABy + 1$ is even, which it is true. We move on to the next step. At step 8 if $p^3 \nmid a_6$ we proceed in the following way, since $p = 2$. Set $k \leftarrow 2$ and compute new $a_1, \ldots, a_6$ with parameters $u_1 = 1, r_1 = 0, s_1 = 0, t_1 = 2$,

$u = 1, r = 1, s = 1, t = 2$ for output.

$$a'_1 = 2, \quad a'_2 = 2, \quad a'_3 = 4,$$
$$a'_4 = 3ABy - 1, \quad a'_6 = 2A^2Bx + 3ABy - 3.$$

If $p^3 \mid a_6$, then keep the same old values:

$$a_1 = a_2 = 2, \quad a_3 = 0$$
$$a_4 = 3ABy + 3, \text{and} \quad a_6 = 2A^2Bx + 3ABy + 1.$$

Now, when does $p^3 \mid a_6$? Since $a_6 = 2A^2Bx + 3ABy + 1$, $p^3 \mid a_6$ if and only if $2A^2Bx + 3ABy \equiv 7 \pmod 8$. When $ABy \equiv 3 \pmod 8$, we must have that $2A^2Bx \equiv 6 \pmod 8$, while when $ABy \equiv 7 \pmod 8$ we must have then that $2A^2Bx \equiv 2 \pmod 8$. We have four cases then:

IV.2.1 $2A^2Bx \equiv 2 \pmod 8$ and $ABy \equiv 3 \pmod 8$. In this case $p^3 \nmid a_6$, so we use the new coefficients.

IV.2.2 $2A^2Bx \equiv 2 \pmod 8$ and $ABy \equiv 7 \pmod 8$. In this case $p^3 \mid a_6$, we keep the old coefficients.

IV.2.3 $2A^2Bx \equiv 6 \pmod 8$ and $ABy \equiv 3 \pmod 8$. In this case $p^3 \mid a_6$, so we use the old coefficients.

IV.2.4 $2A^2Bx \equiv 6 \pmod 8$ and $ABy \equiv 7 \pmod 8$. In this case $p^3 \nmid a_6$, therefore we use the new coefficients.

First let us take a look at what happens with $v_2(Cz^n)$. So far we know that $v_2(Cz^n) \geq 2$. Let us see if we can make a distinction between $v_2(Cz^n) = 2$ and

≥ 3. If we have that $v_2(Cz^n) \geq 3$ then we have that

$$\begin{aligned} v_2(Cz^n) \geq 3 &\iff Ax^2 + By^3 \equiv 0 \pmod 8 \\ &\iff A + By \equiv 0 \pmod 8 \\ &\iff 1 + ABy \equiv 0 \pmod 8 \\ &\iff ABy \equiv 7 \pmod 8. \end{aligned}$$

So for cases **IV.2.2** and **IV.2.4** we have $v_2(Cz^n) \geq 3$ while for the remaining cases we have $v_2(Cz^n) = 2$. We turn our attention first to the case **IV.2.1**

In this case we have that

$$v_2(ABxy) = 0, \quad 2A^2Bx \equiv 2 \pmod 8, \quad ABy \equiv 3 \pmod 8$$
$$v_2(Cz^n) = 2, \quad v_2(c_4) = 4, \quad v_2(c_6) = 6 \text{ and } \quad v = 8.$$

Since $p^3 \nmid a_6$, we have the new coefficients:

$$a_1 = a_2 = 2,\ a_3 = 4,\ a_4 = 3ABy - 1 \text{ and } a_6 = 2A^2Bx + 3ABy - 3.$$

Remember that for output we have $u = r = s = 1$ and $t = 2$. We now move on to step 9 At this point we must have $p \mid a_2$, $p^2 \mid a_4$ and $p^3 \mid a_6$, which is true according to the equalities that we have for this case. Set $P = X^3 + a_{2,1}X^2 + a_{4,2}X + a_{6,3}$. From the equalities for this case we have that $a_{2,1} = 1$, and $a_{4,2} \equiv 0 \pmod 2$. Let us see the values for $a_{6,3} \pmod 2$. An easy calculation show us that $a_6 \equiv 0 \pmod{16}$ if and only if we have

$$(2A^2Bx, 3ABy) \in \{(2, 11), (10, 3)\} \pmod{16},$$

and that $a_6 \equiv 8 \pmod{16}$ if and only if we have

$$(2A^2Bx, 3ABy) \in \{(2, 3), (10, 11)\} \pmod{16},$$

For the first case we obviously have that $a_{6,3} \equiv 0 \pmod 2$ and for the second one $a_{6,3} \equiv 1 \pmod 2$. Now consider that $a_{6,3} \equiv 1 \pmod 2$, therefore our polynomial $P \equiv X^3 + X^2 + 1 \pmod 2$, which has simple roots in $\overline{\mathbb{F}}_2$. So $f_2 = v - 4 = 4$, and we are in case Tate 6^*. To prove this, as before, we need to see if there is exists $r \in \mathbb{Z}$ such that $v_2(b_8(r)) \geq 5$. If not we are in case 6^* otherwise, there will be a $t \in \mathbb{Z}$ such that $a_6(r,t) \equiv 0 \pmod 8$. We are in case 6^* if for that $t, a_6(r,t) \equiv 8 \pmod{16}$. Now when $r \equiv 1 \pmod 4$, $v_2(b_8(r)) \geq 5$, and we see that for $a_6(r,t) \equiv 0 \pmod 8$ if $t \equiv 2 \pmod 4$. Consider now the case when $a_{6,3} \equiv 0 \pmod 2$, we have then $P \equiv X^3 + X^2 \equiv X^2(X+1) \pmod 2$, which has a root in $a = 0$ of multiplicity two in $\mathbb{F}_2$. Move to step 10. Since $a = 0$ and is a double root, we move on to step 16. Set $n \leftarrow 0$ and $f_2 \leftarrow v - 5 - n$. Proceed to the next step. In step 17 we start by setting $P = X^2 + a_{3,2}X - a_{6,4}$. Since $a_{3,2} = 1$, we have that $P \equiv X^2 + X + 1 \pmod 2$ or $P \equiv X^2 + X \equiv X(X+1) \pmod 2$, which both have simple roots over $\overline{\mathbb{F}}_2$. So $f_2 = v - 5 = 3$, corresponding to case Tate 7^* according do Papadopoulos' table. To verify this, there must be an $r \in \mathbb{Z}$ such that $v_2(b_8(r)) \geq 5$ and a for such r there is no such $s \in \mathbb{Z}$ such that $a_2(r,s) \equiv 0 \pmod 4$. Using `MAGMA` we verify that $v_2(b_8(r))$ is verified when $r \equiv 1 \pmod 4$, therefore there is no such $s \in \mathbb{Z}$ such that $a_2(r,s) \equiv 3r - s^2 \equiv 0 \pmod 4$.

We are done with case **IV.2.1** Move on to the next case, **IV.2.2**. The situation in this case is the following:

$$v_2(ABxy) = 0, \quad 2A^2Bx \equiv 2 \pmod 8, \quad ABy \equiv 7 \pmod 8$$

$$v_2(Cz^n) \geq 3 \quad v_2(c_4) = 4, \quad v_2(c_6) = 6 \text{ and } \quad v \geq 9.$$

We also have seen that $p^3 \nmid a_6$ so we keep the old coefficients, that are:

$$a_1 = a_2 = 2, \quad a_3 = 0, \quad a_4 = 3ABy + 3, \text{ and } \quad a_6 = 2A^2Bx + 3ABy + 1,$$

with $u = r = s = 1, t = 0$ accumulated.

We proceed to step 9. We have at this point $p \mid a_2, p^2 \mid a_4$ and $p^3 \mid a_6$, As before, set $P = X^3 + a_{2,1}X^2 + a_{4,2}X + a_{6,3}$. It's easy to see that $a_{2,1} = 1$ and $a_{4,2} \equiv 0 \pmod 2$. Let us look at $a_{6,3}$, it's easy to see that $a_{6,3} \equiv 0 \pmod 2$ if and only if $(2A^2Bx, ABy) \equiv (10, 7), (2, 15) \pmod{16}$, and also that $a_{6,3} \equiv 1 \pmod 2$ if and only if $(2A^2Bx, ABy) \equiv (2, 7), (10, 15) \pmod{16}$. Let us consider in first place $a_{6,3} \equiv 1 \pmod 2$. In this case we have that $P \equiv X^3 + X^2 + 1 \pmod 2$ which has simple roots over $\overline{\mathbb{F}}_2$. So we have that $f_2 = v - 4 \geq 5$, which by the previous table we are in case 6, and $v = 9$. In fact running a little program in MAGMA it's easy to prove that when $ABxy \equiv 1 \pmod 2$ and $(2A^2Bx, ABy) \equiv (2, 7), (10, 15) \pmod{16}$, we have that $v_2(Cz^n) = 3$, therefore $v = 6 + v_2(Cz^n) = 9$. Consider now the case when $a_{6,3} \equiv 0 \pmod 2$. For this we have that $P \equiv X^3 + X^2 \equiv X^2(X + 1) \pmod 2$, which clearly has a double root, $a = 0$ over $\mathbb{F}_2$. For this fact we proceed to step 16. Set $n \leftarrow 0$ and $f_2 = v - 5 - n$. Move on to the next step. As before in step 17 we start by setting $P = X^2 + a_{3,2}X - a_{6,4}$. Since $a_3 = 0$, then $a_{3,2} = 0$, implying that $P \equiv X^2+1 = (X+1)^2 \pmod 2$ or $P \equiv X^2 \pmod 2$, both of which have double roots, $r_0 = a_{6,4}$. We have that $r_0 = 0$, when $a_6 \equiv 0 \pmod{32}$, that is, when $(2A^2Bx, ABy) \equiv (2, 31), (10, 7), (18, 15), (26, 23) \pmod{32}$, and that $r_0 = 1$, when $(2A^2Bx, ABy) \equiv (2, 15),\ (10, 23), (18, 31), (26, 7) \pmod{32}$ Move to the next step. In step 18 we set $n \leftarrow n + 1$. Using $u' = 1, r' = s' = 0$ and $t' = r_0p^2$, with $u = r = s = 1$ and $t = r_0p^2$ for output, calculate the new coefficients:

$$a'_1 = 2, \quad a'_2 = 2, \quad a'_3 = 2r_0p^2,$$
$$a'_4 = 3ABy + 3 - 2r_0p^2, \quad a'_6 = 2A^2Bx + 3ABy + 1 - r_0p^4.$$

Move on to step 19. Set $P = a_{2,1}X^2 + a_{4,3}X + a_{6,5}$. It's easy to see that $a_{2,1} = 1$. Now let us take a look at the value of $a_{4,3} \pmod 2$. If $r_0 \equiv 0$ then $a_{4,3} \equiv 0 \pmod 2$ if and only if $ABy \equiv 15 \pmod{16}$, otherwise we will have $a_{4,3} \equiv 1 \pmod 2$. When $r_0 = 1$, then $a_{4,3} \equiv 0 \pmod 2$, if and only if $ABy \equiv 7 \pmod{16}$. So when $(2A^2Bx, ABy) \equiv (2, 31), (10, 23), (18, 15), (26, 7) \pmod{32}$ our polynomial P will be of the form $P \equiv X^2 + a_{6,5} \pmod 2$, having a double root at $r_1 = a_{6,5}$. When $(2A^2Bx, ABy) \equiv (2, 15), (10, 7), (18, 31), (26, 23) \pmod{32}$, our polynomial is of the form $P \equiv X^2 + X + a_{6,5} \pmod 2$, which has simple roots over $\mathbb{F}_2$. So for this case we are finished with $f_2 = v - 5 - n = v - 6$. From Papadopoulos' table we see that we are in case 7^*, with $v = 10$, meaning that $v_2(Cz^n) = 4$. Using `MAGMA`, we confirm that when $(2A^2Bx, ABy) \equiv (2, 15), (10, 7), (18, 31), (26, 23) \pmod{32}$, then we must have $v_2(Cz^n) = 4$. For the remaining cases we move on to step 20. Let r_1 be the double root of P modulo 2. Using the formulas from Table 5.1 and the parameters $u' = 1, r' = r_1p^2, u' = t' = 0$ compute the new coefficients a_1, a_2, a_3, a_4, a_6, $u = 1, r = 1 + r_1p^2, s = 1, t = (r_0 + r_1)p^2$.

$$a'_1 = 2, \quad a'_2 = 3r_1p^4 - 1, \quad a'_3 = 2(r_0 + r_1)p^2,$$
$$a'_4 = 3ABy + 3r_1p^4 - 2(r_0 + r_1)p^2,$$
$$a'_6 = 2A^2Bx + 3r_1p^2ABy + r_1p^6 - (r_0 + r_1)p^4.$$

Move to the next step. Now in step 21 we set $q \leftarrow qp$ and $n \leftarrow n + 2$. We go back to step 17. Set $P = X^2 + a_{3,3}X - a_{6,5}$. It is easy to see that $a_{3,3} \equiv 0$ or $1 \pmod 2$, depending on r_0 and r_1. When $a_{3,3} \equiv 1 \pmod 2$ then P has simple roots and we are finished, that is, $f_2 = v - 5 - n = v - 7$. By using Papadopoulos table we see that we are in case 7^* with $v = 11$ and $f_2 = 4$ or in case 10^* with $v = 10$ and $f_2 = 3$. But using `MAGMA` we see that for these

cases we can only have $v \geq 11$, so it's case 7^*. When $a_{3,3} \equiv 0 \pmod 2$, we have as before that P will have a double root modulo 2, $r_2 = a_{6,5} \pmod 2$. Well, if we decide to do one more step we will see that this process seems to be going on forever. How do we stop it? Well, we will use the information that we have from Papadopoulos' table and from the case we are on. First, using MAGMA we can see that, when $(2A^2Bx, ABy) \equiv (2, 15), (10, 7) \pmod{16}$ we have that $v_2(Cz^n) \geq 4$. So looking at the Papadopoulos' table 5.4, we have that we can only be in case 7^* or in case 9^* or in 10^*. Looking at the algorithm, we can see that the Kodaira type is I_v^*, and looking at the Papadopoulos' table we have that for this Kodaira type and for the values of $v_2(c_4), v_2(c_6)$ and v we must have case Tate 7^*. To prove that we are in this case we just need to find $r \in \mathbb{Z}$ such that $v_2(b_8(r)) \geq 5$ and that for such r there is no s such that $a_2(r, s) \equiv 0 \pmod 4$. Now we have that $a_2(r, s) = 3r^2 - s^2$. So $a_2(r, s) \not\equiv 0 \pmod 4$, only when $r \equiv 1$ or $2 \pmod 4$. We use MAGMA to find possible r such that $v_2(b_8(r)) \geq 5$, and we see that this is only possible when $r \equiv 1 \pmod 4$, therefore we have that we are in Tate's case 7^* so we have that $f_2 = 4$. Also using MAGMA we see that $v_2(Cz^n) \geq 4$ for all cases and that, we only have the $v_2(Cz^n) = 4$ when

$$(2A^2Bx, ABy) \equiv (2, 15), (10, 7), (18, 31), (26, 23) \pmod{32}.$$

We have $v_2(Cz^n) = 5$ when $(2A^2Bx, ABy)$ is one of the following tuples $\pmod{64}$

$$(2, 31), (10, 23), (18, 47), (26, 39), (34, 63), (42, 55), (50, 15), (58, 7),$$

and $v_2(Cz^n) \geq 6$, when $(2A^2Bx, ABy) \pmod{64}$ is one tuple of the following list

$$(2, 63), (10, 55), (18, 15), (26, 7), (34, 31), (42, 23), (50, 47), (58, 39),$$

And with this we are finished with the case **IV.2.2**.

We move on to the case **IV.2.3** First of all, let us recall which are the conditions that we have for this case,

$$v_2(ABxy) = 0, \quad 2A^2Bx \equiv 6 \pmod 8, \quad ABy \equiv 3 \pmod 8$$
$$v_2(Cz^n) = 2 \quad v_2(c_4) = 4, \quad v_2(c_6) = 6 \text{ and } \quad v = 8.$$

We also have $p^2 \mid a_6$, so keep the old coefficients, that are

$$a_1 = a_2 = 2, \quad a_3 = 0, \quad a_4 = 3ABy + 3, \text{ and } \quad a_6 = 2A^2Bx + 3ABy + 1,$$

with $u = r = s = 1$ and $t = 0$ for output.

We move to step 9. As always, at this point we have that $p^i \mid a_{2i}$, with $i \in \{1, 2, 3\}$. Set $P = X^3 + a_{2,1}X^2 + a_{4,2}X + a_{6,3}$ We can see that $a_{2,1} = 1$ and that $a_{4,2} \equiv 1 \pmod 2$, since $a_4 \equiv 4 \pmod 8$. So $P \equiv X^3 + X^2 + X \equiv X(X^2 + X + 1) \pmod 2$, which has simple roots over $\overline{\mathbb{F}}_2$ if $a_{6,3} \equiv 0 \pmod 2$ or $P \equiv X^3 + X^2 + X + 1 \equiv (X + 1)^3 \pmod 2$, which has a root, $a = 1$ of multiplicity 3. It is possible to see that $a_6 \equiv 0 \pmod{16}$ if and only if $(2A^2Bx, ABy) \equiv (6, 3), (14, 11) \pmod{16}$ and that $a_{6,3} \equiv 1 \pmod 2$ if and only if $(2A^2Bx, ABy) \equiv (6, 11), (14, 3) \pmod{16}$. So when $a_{6,3} \equiv 0 \pmod 2$, that is when $(2A^2Bx, ABy) \equiv (6, 3), (14, 11) \pmod{16}$, our polynomial P has simple roots, so we are finished with $f_2 = v - 4 = 4$, Tate's case 6^*. We see that $v_2(b_8(r)) \geq 5$ has solutions if and only if $r \equiv 3 \pmod 4$, and that $v_2(a_6(r, t)) \geq 3$ if and only if when $t \equiv 2 \pmod 4$, and in this case the congruence becomes and equality equal to 3. When $a_{6,3} \equiv 1 \pmod 2$, that is when $(2A^2Bx, ABy) \equiv (6, 11), (14, 3) \pmod{16}$, we have that our polynomial P has a triple root $a = 1$. So we proceed to step 10. We change the equation with parameters $u_1 = 1, r_1 = 2, s_1 = t_1 = 0$, for output we have $u = 1, r = 3, s = 1, t = 2$. So our new

coefficients are:

$$a'_1 = 2, \quad a'_2 = 8, \quad a'_3 = 4,$$
$$a'_4 = 3ABy + 23, \quad a'_6 = 2A^2Bx + 9ABy + 23.$$

Proceed now to step 11. Now we must have $p^2 \mid a_3 = 4$ and $p^4 \mid a_6$, which is true for both cases. Set then, $P = X^2 + a_{3,2}X + a_{6,4}$. Since $a_{3,2} \equiv 1 \pmod 2$ and X^2+X or X^2+X+1 have simple roots on $\overline{\mathbb{F}}_2$, we are finished with $f_2 = v-6 = 2$, that corresponds to Tate's case 8^* on Papadopoulos' table. It's easy to verify that $v_2(b_8(r)) \geq 5$ if and only if $r \equiv 3 \pmod 4$, so this implies that $a_2(r,s) \equiv 0 \pmod 4$ only when s is odd, so we are in Tate case 8^*. And we are finished with case **IV.2.3**.

We move now to case **IV.2.4** Let us recall the conditions and the specific values we have for this case:

$$v_2(AxBy) = 0, \quad 2A^2Bx \equiv 6 \pmod 8, \quad ABy \equiv 7 \pmod 8,$$
$$v_2(Cz^n) \geq 3, \quad v_2(c_4) = 4, \quad v_2(c_6) = 6, \text{ and } \quad v \geq 9.$$

We also have that $p^3 \nmid a_6$, so for that reason we choose the new coefficients:

$$a_1 = a_2 = 2, \quad a_3 = 4, \quad a_4 = 3ABy - 1, \text{ and}$$
$$a_6 = 2A^2Bx + 3ABy - 3,$$

with $u = r = s = 1$ and $t = 2$ for output.

The same as in case **IV.2.2**. We proceed now to step 9. At this point we have that $p^i \mid a_{2i}$, for $i \in \{1,2,3\}$. Set $P = X^3 + a_{2,1}X^2 + a_{4,2}X + a_{6,3}$. It is easy to see that $a_{2,1} = 1$ and that $a_{4,2} \equiv 1 \pmod 2$, since $a_4 \equiv 4 \pmod 8$. Therefore we have that, or $P \equiv X^3+X^2+X \equiv X(X^2+X+1) \pmod 2$, which has simple roots over $\overline{\mathbb{F}}_2$, when $a_{6,3} \equiv 0 \pmod 2$ or that $P \equiv X^3+X^2+X+1 \equiv (X+1)^3$

$(\mathrm{mod}\ 2)$,which has a triple root on $a = 1$, when $a_{6,3} \equiv 1\ (\mathrm{mod}\ 2)$. Now $a_{6,3} \equiv 0\ (\mathrm{mod}\ 2) \iff a_6 \equiv 0\ (\mathrm{mod}\ 16)$. This is verified when $(2A^2Bx, ABy) \equiv (6, 15), (14, 7)\ (\mathrm{mod}\ 16)$. On the other hand when $a_{6,3} \equiv 1\ (\mathrm{mod}\ 2)$ we have that $(2A^2Bx, ABy) \equiv (6, 7), (14, 15)\ (\mathrm{mod}\ 16)$. So for $a_{6,3} \equiv 0\ (\mathrm{mod}\ 2)$ we are finished and $f_2 = v - 4 \geq 5$, so it can only be Tate's case 6, which implies that $v = 9$, by using MAGMA we confirm that when $(2A^2Bx, ABy) \equiv (6, 15), (14, 7)\ (\mathrm{mod}\ 16)$, we have that $v_2(Cz^n) = 3$. Now when $a_{6,3} \equiv 1\ (\mathrm{mod}\ 2)$, we move to step 10, with $(2A^2Bx, ABy) \equiv (6, 7), (14, 15)\ (\mathrm{mod}\ 16)$. Using $u_1 = 1, r_1 = 1, s_1 = t_1 = 0$, we change coefficients, with $u = 1, r = 3, s = 1, t = 4$ for output. So we have that

$$a'_1 = 2, \quad a'_2 = 8, \quad a'_3 = 8,$$
$$a'_4 = 3ABy + 19, \quad a'_6 = 2A^2Bx + 9ABy + 11$$

Since $a = 1$ is a root of multiplicity 3 we move to step 11. At this point $p^2 \mid a_3$ and $p^4 \mid a_6$. So set $P \equiv X^2 + a_{3,2}X + a_{6,4}$. Since $a_{3,2} \equiv 0\ (\mathrm{mod}\ 2)$ then $P \equiv (X + 1)^2\ (\mathrm{mod}\ 2)$ or $P \equiv X^2\ (\mathrm{mod}\ 2)$ both have roots of multiplicity 2. The root depends on the congruence $a_{6,4}\ (\mathrm{mod}\ 2)$. We have that $a_{6,4} \equiv 0\ (\mathrm{mod}\ 2)$ when $(2A^2Bx, ABy) \equiv (6, 23), (14, 15), (22, 7), (30, 31)\ (\mathrm{mod}\ 32)$. On the other hand, we have that $a_{6,4} \equiv 1\ (\mathrm{mod}\ 2)$ when $(2A^2Bx, ABy) \equiv (6, 7), (14, 31), (22, 23), (30, 15)\ (\mathrm{mod}\ 32)$. From now on we will divide in two cases:

IV.2.4.1 $(2A^2Bx, ABy) \equiv (6, 23), (14, 15), (22, 7), (30, 31) \quad (\mathrm{mod}\ 32)$.

IV.2.4.2 $(2A^2Bx, ABy) \equiv (6, 7), (14, 31), (22, 23), (30, 15) \quad (\mathrm{mod}\ 32)$.

We will start with case **IV.2.4.1**. Since $a = 0$, we move on to step 13. If $p^4 \mid a_4$ set $f_2 = v - 7$. So we have $a_4 \equiv 3ABy + 19 \equiv 3ABy + 3$

$(\mathrm{mod}\ 16)$. So if $ABy \equiv 7\ (\mathrm{mod}\ 16)$ then $a_4 \equiv 8\ (\mathrm{mod}\ 16)$, while $ABy \equiv 15\ (\mathrm{mod}\ 16)$ then $a_4 \equiv 0\ (\mathrm{mod}\ 16)$. So for $(2A^2Bx, ABy) \equiv (6, 23), (22, 7)\ (\mathrm{mod}\ 32)$ we are finished, and $f_2 = v - 7 \geq 2$. Since $v - 7 \geq 3$ we have that $v \geq 10$. So it can only be 7^* with $v = 11$ and $f_2 = 4$ or 9^* with $f_2 = 3$ and $v = 10$. It's easy see $v_2(b_8(r)) \geq 5 \iff r \equiv 3\ (\mathrm{mod}\ 4)$, so $a_2(r, s) \equiv 0\ (\mathrm{mod}\ 4)$ has a solution, just consider $s \equiv 1\ (\mathrm{mod}\ 2)$. So we are in case in 9^*. We could also see that $v_2(Cz^n) = 4$ for this case. For the remaining case, $(2A^2Bx, ABy) \equiv (14, 15), (30, 31)\ (\mathrm{mod}\ 32)$ we move on to the next step. In step 14 we need to know if $p^6 \mid a_6$ or not. If not then $f_2 = v - 8$. Now when do we have $a_6 \equiv 0\ (\mathrm{mod}\ 64)$? Since we have that $(2A^2Bx, ABy) \equiv (14, 15, (30, 31)\ (\mathrm{mod}\ 32)$ and $a_6 = 2A^2Bx + 9ABy + 11$, we have that $a_6 \equiv 0\ (\mathrm{mod}\ 64)$ if and only if $(2A^2Bx, ABy) \equiv (14, 47), (30, 31), (46, 15), (62, 63)\ (\mathrm{mod}\ 64)$, and on the other hand we have that $p^6 \nmid a_6$ when $(2A^2Bx, ABy) \equiv (14, 15),\ (30, 63), (46, 47), (62, 31)\ (\mathrm{mod}\ 64)$, for this case we have that $f_2 = v - 8 \geq 1$. By Papadopoulos table we have that $v - 8 \geq 3$ that is $v \geq 11$, so we are in case Tate 7^* with $f_2 = 4$ and $v \geq 12$ or in case Tate 10^* with $f_2 = 3$ and $v = 11$. Using `MAGMA` once again we see that when $(2A^2Bx, ABy) \equiv (14, 15)$, $(30, 63), (46, 47), (62, 31)\ (\mathrm{mod}\ 64)$, $v_2(Cz^n) = 5$ which implies that $v = 11$, so we must be in Tate's case 10^*. We just need to find $r \in \mathbb{Z}$ such that $v_2(b_8(r)) \geq 5$, which is true when $r \equiv 3\ (\mathrm{mod}\ 4)$, and so since $a_2(r, s) \equiv 0\ (\mathrm{mod}\ 4)$, take $s \equiv 1\ (\mathrm{mod}\ 2)$, we have proved that we are in Tate's case 10^*. For the remaining case, $(2A^2Bx, ABy) \equiv (14, 47), (30, 31), (46, 15), (62, 63)\ (\mathrm{mod}\ 64)$, we move on to step 15. Using once again the formulas given in Table 5.1 with parameters $u_1 = 2, r_1 = 0, s_1 = 0, t_1 = 0$,(for output we have $u = 2, r = 3, s = 1, t = 4$) we

Table 5.6: $v_2(\Delta) = 12$

m	2	3	4	5	6	≥ 7
$v_2(z)$	3	2	1	1	1	0
$v_2(C)$	0	0	2	1	0	6

.

compute the new coefficients.

$$a_1' = 1, \quad a_2' = 2, \quad a_3' = 1,$$
$$a_4' = (3ABy + 19)/16, \quad a_6' = (2A^2Bx + 9ABy + 11)/64$$

We have that $v \leftarrow v - 12 = v_2(C) + nv_2(z) - 6$, since $\Delta \leftarrow \Delta/2^{12}$, we have that $v_2(c_4) = v_2(c_6) = 0$, since $c_4 \leftarrow c_4/2^4$ and $c_6 \leftarrow c_6/2^6$. So by Papadopoulos' table we have that before changing the coefficients we were in a non minimal case, now with the new coefficients, we are for sure in a minimal case since both $v_2(c_4) = v_2(c_6) = 0$.

We now proceed to step 2. If $v = 0$ then $f_2 = 0$. Now this happens when $v_2(C) + nv_2(z) = 6$. Since $n \geq 2$ and $v_2(C) \leq n - 1$ we have the following cases where $v = 0$. So when $(2A^2Bx, ABy) \equiv (14, 47), (30, 31), (46, 15), (62, 63) \pmod{64}$ and m, z and C are as in the table we are done with $f_2 = 0$, Tate's case 1. For the rest we move on to step 3. Since $p \nmid a_1^2 + 4a_2 = 1 + 8 = 9$, then set $f_2 = 1$, which corresponds in Papadopoulos' table to Tate's case 2. And we are done with case **IV.2.4.1**, we move now to case **IV.2.4.2**.

For this case we have $(2A^2Bx, ABy) \equiv (6, 7), (14, 31), (22, 23), (30, 15) \pmod{32}$. Since $a_{6,4} \equiv 1 \pmod 2$, we have that our polynomial P defined at step 11, is such that $P \equiv (X + 1)^2 \pmod 2$. So it has a double root in $a = 1$. Therefore we move on to step 12. Using parameters $u_1 = 1, r_1 = 0, s_1 = 0, t_1 = 4$,

for output we will have $u = 1, r = 3, s = 1, t = 8$ we compute the new coefficients:

$$a_1' = 2, \quad a_2' = 8, \quad a_3' = 16,$$
$$a_4' = 3ABy + 11, \quad a_6' = 2A^2Bx + 9ABy - 37.$$

Proceed now to step 13. If $p^4 \mid a_4$ set $f_2 = v - 7$. So we have $a_4 = 3ABy + 11$. So if $ABy \equiv 7 \pmod{16}$ then $a_4 \equiv 0 \pmod{16}$, while $ABy \equiv 15 \pmod{16}$ then $a_4 \equiv 8 \pmod{16}$. So for $(2A^2Bx, ABy) \equiv (14, 31), (30, 15) \pmod{32}$ we are finished, and $f_2 = v - 7 \geq 2$. Since $v - 7 \geq 3$ we have that $v \geq 10$. So it can only be 7^* with $v = 11$ and $f_2 = 4$ or 9^* with $f_2 = 3$ and $v = 10$. So we just need to have an $r \in \mathbb{Z}$ such that $v_2(b_8(r)) \geq 5$. If $r \equiv 1, 2 \pmod{4}$ then we are in case 7^* otherwise, when $r \equiv 0, 3 \pmod{4}$ we are in case 9^*, since for the first set of congruences we will not find $s \in \mathbb{Z}$ such that for the given r, $a_2(r, s) \equiv 0 \pmod{4}$, while for the second set of congruences we will. Using `MAGMA` we see that the congruence $v_2(b_8(r)) \geq 5$ is satisfied only with $r \equiv 3 \pmod{4}$ so it's case 9^*. We could also see that $v_2(Cz^n) = 4$ for this case. For the remaining case, $(2A^2Bx, ABy) \equiv (6, 7), (22, 23) \pmod{32}$ we move on to the next step. As before, in step 14, we want to know if $p^6 \mid a_6$ or not. If not then $f_2 = v - 8$. Now when do we have $a_6 \equiv 0 \pmod{64}$? Since we have that $(2A^2Bx, ABy) \equiv (6, 7), (22, 23) \pmod{32}$ and $a_6 = 2A^2Bx + 9ABy - 37$, we have that $a_6 \equiv 0 \pmod{64}$ if and only if $(2A^2Bx, ABy) \equiv (6, 39), (22, 23), (38, 7), (54, 55) \pmod{64}$, and on the other hand we have that $p^6 \nmid a_6$ when $(2A^2Bx, ABy) \equiv (6, 7), (22, 55), (38, 39), (54, 23) \pmod{64}$, for this case we have that $f_2 = v-8 \geq 1$. By Papadopoulos table we have that $v-8 \geq 3$ that is $v \geq 11$, so we are in case Tate 7^* with $f_2 = 4$ and $v \geq 12$ or in case de Tate 10^* with $f_2 = 3$ and $v = 11$. Using `MAGMA` once again we see that $v = 11$, since that when we have $(2A^2Bx, ABy) \equiv (6, 7), (22, 55), (38, 39), (54, 23) \pmod{64}$,

we have that $v_2(Cz^n) = 5$, so we can only be in Tate's case 9^*. For the remaining case, $(2A^2Bx, ABy) \equiv (6, 39), (22, 23), (38, 7), (54, 55) \pmod{64}$, we move on to step 15. Using once again the formulas given in Table 5.1 with parameters $u_1 = 2, r_1 = 0, s_1 = 0, t_1 = 0$,(for output we have $u = 2, r = 3, s = 1, t = 8$) we compute the new coefficients.

$$a_1' = 1, \quad a_2' = 2, \quad a_3' = 2,$$
$$a_4' = (3ABy + 11)/16, \quad a_6' = (2A^2Bx + 9ABy - 37)/64$$

And as before, we have that $v \leftarrow v - 12 = v_2(C) + nv_2(z) - 6$, since $\Delta \leftarrow \Delta/2^{12}$, we have that $v_2(c_4) = v_2(c_6) = 0$, since $c_4 \leftarrow c_4/2^4$ and $c_6 \leftarrow c_6/2^6$. As we have seen in a similar case above, by Papadopoulos' table we see that before changing the coefficients we were in a non minimal case, now with the new coefficients, we are for sure in a non-minimal case since both $v_2(c_4) = v_2(c_6) = 0$. We now proceed to step 2. If $v = 0$ then $f_2 = 0$. Now this happens when $v_2(C) + nv_2(z) = 6$. Since $n \geq 2$ and $v_2(C) \leq n - 1$, the cases where $v = 0$ are presented in Table 5.6. So when $(2A^2Bx, ABy) \equiv (6, 39), (22, 23), (38, 7), (54, 55) \pmod{64}$ and m, z and C are as in the table we are done with $f_2 = 0$, Tate's case 1. For the rest we move on to step 3. Since $p \nmid a_1^2 + 4a_2 = 1 + 8 = 9$, then set $f_2 = 1$, which corresponds in Papadopoulos' table to Tate's case 2. And we are finished with case **IV.2.4.2** as well with the case **IV.2** We move now to the case **IV.3** In this case we have that $v_2(x) \geq 1$ and $ABy \equiv 1 \pmod{4}$, which implied that $p^2 \mid a_6$, just to recall here are the coefficients at this point :

$$a_1 = a_2 = 2, \quad a_3 = 0, \quad a_4 = 3ABy + 3, \text{ and}$$
$$a_6 = 2A^2Bx + 3ABy + 1.$$

Remember also that we have $v_2(c_4) = 4, v_2(c_6) \geq 7$ and $v = 6$.

We now move to step 6. First, we compute $b_8 = b_8 + 3b_6 + 3b_4 + 3 = -9A^2B^2y^2 + 24A^2Bx + 18ABy + 3$. If $p^3 \nmid b_8$ then set $f_2 = v - 1$. Now $b_8 \equiv 0 \pmod 8$ is equivalent to

$$\begin{aligned} -(3ABy)^2 + 2ABy + 3 \equiv 0 \pmod 8 &\iff 2 + 2ABy \equiv 0 \pmod 8 \\ &\iff 2ABy \equiv 6 \pmod 8 \\ &\iff ABy \equiv 3 \pmod 4, \end{aligned}$$

which is false, so $p^3 \nmid b_8$ and we are done with $f_2 = v - 1 = 5$, Tate's case 4^*. Since for $r \in \mathbb{Z}$ such that $r \equiv 1 \pmod 4$ we have that $2 \nmid a_4 + r^2$, and for that r $p^3 \nmid b_8(r)$, we see that it's Tate's case 4^*. So case **IV.3** is done. We move now to case **IV.4**, where we have that

$$\begin{gathered} v_2(x) \geq 1, \quad ABy \equiv 3 \pmod 4, p^2 \nmid a_6 \\ v = 6 \quad v_2(c_4) = 4, \quad v_2(c_6) \geq 7 \\ a_1 = a_2 = 2, \quad a_3 = 0, \quad a_4 = 3ABy + 3, \text{ and} \\ a_6 = 2A^2Bx + 3ABy + 1. \end{gathered}$$

Since $p^2 \nmid a_6$ we have that $f_2 = v = 6$, which by Papadopoulos' table we are i case 3^*. It's easy to see that $a_4 + r^2$ is even when r is odd and with t even we have that $t^2 + a_4a_2 - a_6$ is even too. For this values of r and t do we have that $v_2(a_6(r,t)) \geq 2$? Remember that for this case $a_6(r,t) = a_6 + ra_4 + r^3 - t^2$. Since $4 \mid a_6$ and $4 \mid t^2$ we have that if $4 \mid a_6(r,t)$ then $4 \mid 3ABy + 1$, since r is odd, but then $ABy \equiv 1 \pmod 4$, which is not our assumption, then we are in case 3^*. So we are finished for $p = 2$.

5.2.3 Exponent for $p = 3$

Now we move on to the prime $p = 3$. We start by setting $u \leftarrow 1, r \leftarrow 0, s \leftarrow 0, t \leftarrow 0$,

$$v = v_3(\Delta) = \begin{cases} 6 + 3v_3(A) & \text{if } 3 \mid Ax, \\ 6 + 2v_3(B) & \text{if } 3 \mid By, \\ 6 + v_3(C) + nv_3(z) & \text{if } 3 \mid Cz, \\ 3 & \text{otherwise.} \end{cases} \tag{5.7}$$

We move on to the next step. In step 2 if $v = 0$ then set $f_3 = 0$ and we are finished. From what we can see from above, $v \geq 3$. So move on to the next step. For step 3 if $p \nmid b_2$ then set $f_3 = 1$ and we are finished. Since $b_2 = 0$, we have to move on to the next step. In step 4 set $r_1 \equiv -b_6 \pmod 3, s_1 \equiv a_1 \pmod 3, t_1 \equiv (a_3 + ra_1) \pmod 3$. With these parameters compute the new $a_1, \ldots, a_6$. Since $a_1 = a_3 = 0$ we have that $s_1 = 0$ and $t_1 = 0$. Now $b_6 = 8A^2Bx \equiv 2A^2Bx \pmod 3$. If $3 \mid ABx$ then $r_1 = 0$. And so, we do not need to change our coefficients. If $3 \nmid ABx$, then we can have $A^2Bx \equiv \pm 1 \pmod 3$. If $A^2Bx \equiv 1 \pmod 3$ we have that $b_6 \equiv 2 \pmod 3$, then $r_1 = 1$. In this case our coefficients will be

$$a_1' = 0, \quad a_2' = 3, \quad a_3' = 0,$$
$$a_4' = 3(ABy + 1), \quad a_6' = 2A^2Bx + 3ABy + 1.$$

If $A^2Bx \equiv 2 \pmod 3$, then $r_1 = 2$. In this case we have the following coefficients

$$a_1' = 0, \quad a_2' = 6, \quad a_3' = 0,$$
$$a_4' = 3(ABy + 4), \quad a_6' = 2A^2Bx + 6ABy + 8.$$

So we have five possible cases

I : $v_3(A) = 1$, so $v_3(b_6) \geq 1$ and $r_1 = 0$;

II : $v_3(B) \geq 1$, so $v_3(b_6) \geq 1$ and $r_1 = 0$;

III : $v_3(A) = 0$ and $v_3(x) \geq 1$, so $v_3(b_6) \geq 1$ and $r_1 = 0$;

IV : $3 \nmid ABx$ and $A^2Bx \equiv 1 \pmod 3$, which implies that $r_1 = 1$;

V : $3 \nmid ABx$ and $A^2Bx \equiv 2 \pmod 3$, so we have that $r_1 = 2$.

We move on to step 5 considering case **I**. So for this case we have $r_1 = s_1 = t_1 = 0$, so we don't change our coefficients.

We proceed to step 5. If $3^2 \nmid a_6$, then set $f_3 = v$ and we are finished. Since we have that $3 \mid A$, then $3^2 \mid 2A^2Bx = a_6$. We proceed then to step 6. If $p^3 \nmid b_8$ then set $f_3 = v - 1$ and we have finished. We have that $b_8 = -9A^2B^2y^2$. Clearly we have that $p^3 \mid b_8$. We proceed to the step 7. If $p^3 \nmid b_6$, then set $f_3 = v - 2$ and we are finished. Now $b_6 = 8A^2Bx$, $v_3(b_6) \geq 3$ if and only if $v_3(A) = 1$ and $v_3(x) \geq 1$. So when we have $v_3(A) = 1$ and $v_3(x) = 0$ we are finished with $f_3 = v - 2 = 4$, Tate's case 5. So we proceed to the next step with the case where $v_3(A) = 1$ and $v_3(x) \geq 1$. We are now in step 8. Does $p^3 \nmid a_6$? Since we have $v_3(A) = 1$ and $v_3(x) \geq 1$ it does, so we move on to the step 9. At this point we must have $p^i \mid a_{2i}$, with $i \in \{1, 2, 3\}$, which it is true. Set $P = X^3 + a_{2,1}X^2 + a_{4,2}X + a_{6,3}$. As we have that $a_2 = 0$ and $v_3(a_4) = 2$, we then have that $a_{2,1} = 0$ and $a_{4,2} \equiv 1, 2 \pmod 3$. Now, $v_3(a_6) \geq 4$ if and only if $v_3(x) \geq 2$. So we have that $a_{6,3} \equiv 0, 1, 2 \pmod 3$. So $P \pmod 3$ can be of the following ones:

- $P \equiv X^3 + X \equiv X(X^2 + 1) \pmod 3$;
- $P \equiv X^3 + X + 1 \equiv (X + 2)(X^2 + X + 1) \pmod 3$;
- $P \equiv X^3 + X + 2 \equiv (X + 1)(X^2 + 2X + 2) \pmod 3$;

- $P \equiv X^3 + 2X \equiv X(X+1)(X+2) \pmod 3$;
- $P \equiv X^3 + 2X + 1 \pmod 3$;
- $P \equiv X^3 + 2X + 1 \pmod 3$.

It is easy to see that in all possibilities for P we have that P has simple roots over $\overline{\mathbb{F}}_3$. So we re finished with $f_3 = v - 4 = 2$, Tate's case 6.

We turn to case **II**, where we have that $v_3(B) \geq 1$, $r_1 = s_1 = t_1 = 0$, so no need to change coefficients, that is our coefficients are:

$$a_1 = a_2 = a_3 = 0,\ a_4 = 3ABy, \text{ and } a_6 = 2A^2Bx.$$

We also have the following information:

$$v_3(c_4) \geq 3, \quad v_3(c_6) \in \{4, 5\} \text{ and } \quad v \in \{5, 7\}$$

We proceed to step 5. If $p^2 \nmid a_6$ then $f_3 = v$. Now $a_6 = 2A^2Bx$, $p^2 \mid a_6 \iff v_3(B) = 2$. So if $v_3(B) = 1$ we have that $f_3 = v = 5$, Tate's case 3. For $v_3(B) = 2$ we move to the next step. For step 6 we compute $b_8 = -(3ABy)^2$, since $v_3(B) = 2$ we have that $p^3 \mid b_8$. Move to step 7. If $p^3 \nmid b_6$, then set $f_3 = v - 2$. Now $b_6 = 8A^2Bx$, and clearly we have that $v_3(b_6) = 2$, so $p^3 \nmid b_6$ and $f_3 = v - 2 = 5$, which by Papadopoulos' table corresponds to Tate's case 5. Case **II** is done, we move on to case **III**.

In this case we have that $v_3(x) \geq 1$ and $v_3(A) = 0$. So $r_1 = 0$ and we don't change coefficients. We also have that $v_3(c_4) = 2$, $v_3(c_6) \geq 4$ and $v = 3$. We proceed now to step 5. If $p^2 \nmid a_6$ then set $f_3 = v$. Since $a_6 = 2A^2Bx$, we have that $p^2 \nmid a_6$ if and only if $v_3(x) = 1$, and in this case $f_3 = v = 3$, Tate's case 3. When we have $v_3(x) \geq 2$, then $p^2 \mid a_6$ and we move on to step 6. Compute now $b_8 = -9A^2B^2y^2$. In this case we have that $v_3(b_8) = 2$, therefore $p^3 \nmid b_8$ and

so $f_3 = v - 1 = 2$, Tate's case 4. And we are done with case **III**. Proceed now to case **IV**.

First of all, let us recall that in this case we have that $v_3(ABx) = 0$, and $A^2Bx \equiv 1 \pmod 3$, so $r_1 = 1$ and we have to change our coefficients. These are our new coefficients:

$$a_1 = 0, \quad a_2 = 3, \quad a_3 = 0, \quad a_4 = 3ABy + 3, \quad \text{and}$$
$$a_6 = 2A^2Bx + 3ABy + 1.$$

About the values of $v_3(c_4), v_3(c_6)$ and v we have the following cases:

- If $3 \mid y$ then $v_3(c_4) \geq 3, v_3(c_6) = 3$ and $v = 3$.
- If $3 \mid Cz$ then $v_3(c_4) = 2, v_3(c_6) = 3$ and $v \geq 4$.
- If $3 \nmid Cyz$ then $v_3(c_4) = 2, v_3(c_6) = 3$ and $v = 3$.

We move on to the next step. We are now in Step 5. If $p^2 \nmid a_6$, then set $f_3 = v$ and we are finished. $a_6 = 2A^2Bx + 3ABy + 1$, recall that we have $3 \nmid ABx$ and $A^2Bx \equiv 1 \pmod 3$. If $3 \mid y$ then $9 \mid 3ABy$ and so, in order to have $9 \mid a_6$ we must have that $2A^2Bx + 1 \equiv 0 \pmod 9$, that is $A^2Bx \equiv 4 \pmod 9$. If $3 \nmid y$, then $A^2Bx \equiv 1, 4$ or $7 \pmod 9$. Consider first that $A^2Bx \equiv 1 \pmod 9$, then in order to have $a_6 \equiv 0 \pmod 9$ we must have $3ABy \equiv 6 \pmod 9$. Turning now to the case $A^2Bx \equiv 4 \pmod 9$ we get that $3ABy \equiv 0 \pmod 9$ in order to have $p^2 \mid a_6$, which implies that $3 \mid y$. And finally when we have $A^2Bx \equiv 7 \pmod 9$, if we have $a_6 \equiv 0 \pmod 9$ then we have that $3ABy \equiv 3 \pmod 9$. So when $(A^2Bx, 3ABy) \equiv (1,6), (7,3), (4,0) \pmod 9$, we have $p^2 \mid a_6$. On the other hand when we have $(A^2Bx, 3ABy) \equiv (1,0), (1,3), (4,3), (4,6), (7,0), (7,6) \pmod 9$ we have that $p^2 \nmid a_6$, so we have finished for these cases, with $f_3 = v$. By Papadopoulos we can be in case Tate 3 not P_2, with $f_3 = v = 3$ or in case Tate 4,

with $f_3 = v = 4$. Using MAGMA, we see that when $(A^2Bx, 3ABy) \equiv (4,6),(7,6) \pmod 9$ then $v_3(Cz^n) = 1$, while for the other cases $v_3(Cz^n) = 0$, that is, for all the numbers A, x, B, y in $\{0, 1, \ldots, 8\}$ such that assumptions above are verified, we have that $Ax^2 + By^3 \equiv 3$ or $6 \pmod 9$. So for $(A^2Bx, 3ABy) \equiv (4,6),(7,6) \pmod 9$ we are in Tate's case 4. For the remaining ones, to show that we are in case Tate 3 not P_2, we must see that there is no $r \in \mathbb{Z}$ such that

$$r^3 + b_2r^2 + 8b_4r + 16b_6 \equiv 0 \pmod{3^2}.$$

This is easily verified with a simple algorithm implemented on MAGMA. Also using MAGMA we see that when $(A^2Bx, 3ABy) \equiv (4,0),(7,3) \pmod 9$, $v_3(Cz^n) = 0$ implying that $v = 3$ and that when $(A^2Bx, 3ABy) \equiv (1,6) \pmod 9$ then $v_3(Cz^n) \geq 2$, that is $v \geq 5$. We move now to step 6. If $p^3 \nmid b_8$, set $f_3 = v - 1$ and we are finished. We have that $b_8 = -9A^2B^2y^2 + 24A^2Bx + 18ABy + 3$. Now $p^3 \mid b_8 \iff (A^2Bx, 3ABy) \equiv (1,6) \pmod 9$, and so for $(A^2Bx, 3ABy) \equiv (4,0),(7,3) \pmod 9$ we have finished with $f_3 = v - 1 = 2$, and so we are in case Tate 4 P_2. In fact, for these cases we have that the congruence $r^3 + b_2r^2 + 8b_4r + 16b_6 \equiv 0 \pmod 9$ has a solution for some $r \in \mathbb{Z}$. So we are still left with $(A^2Bx, 3ABy) \equiv (1,6) \pmod 9$. Proceed then to step 7. If $p^3 \nmid b_6$ then set $f_3 = v-2$ and we are finished. In this case we have $b_6 = 8A^2Bx+12ABy+4$. So $p^3 \mid b_6$ if and only if $(A^2Bx, 3ABy) \equiv (1,24),(10,6),(19,15) \pmod{27}$. Therefore $p^3 \nmid b_6$ if and only if $(A^2Bx, 3ABy) \equiv (1,6),(1,15)(10,15),(10,24)(19,6),(19,24) \pmod{27}$, so for these case we are finished with $f_3 = v - 2 \geq 3$. By Tate's case 5, with $v = 5$ and $f_3 = 3$. In fact, using MAGMA, it's possible to see that for these cases we have $v_3(Cz^n) = 2$. For the remaining cases we move to step 8. If $p^3 \nmid a_6$, set $k \equiv a_3 \pmod 9$, but since $a_6 = 2A^2Bx + 3ABy + 1$, and we have that $b_6 = 4a_6$, so since $p^3 \mid b_6$ we have that $p^3 \mid a_6$. So we move to

the next step. As before, we now have that $p \mid a_2, p^2 \mid a_4$ and $p^3 \mid a_6$. Set $P = X^3 + a_{2,1}X^2 + a_{4,2}X + a_{6,3}$. We clearly see that $a_{2,1} \equiv 1 \pmod 3$, and that $a_{4,2} \equiv 0, 1, 2 \pmod 3$ if $3ABy \equiv 24, 6, 15 \pmod{27}$ respectively. Now let us take a look at $a_{6,3} \pmod 3$. When we have that $3ABy \equiv 24 \pmod 3$, then

$$a_{6,3} = 0 \pmod 3 \iff (A^2Bx, 3ABy) \equiv (1, 78), (28, 24), (55, 51) \pmod{81}$$
$$a_{6,3} = 1 \pmod 3 \iff (A^2Bx, 3ABy) \equiv (1, 24), (28, 51), (55, 78) \pmod{81}$$
$$a_{6,3} = 2 \pmod 3 \iff (A^2Bx, 3ABy) \equiv (1, 51), (28, 78), (55, 24) \pmod{81}$$

When we have that $3ABy \equiv 6 \pmod{27}$, we have that

$$a_{6,3} = 0 \pmod 3 \iff (A^2Bx, 3ABy) \equiv (10, 60), (37, 6), (64, 33) \pmod{81}$$
$$a_{6,3} = 1 \pmod 3 \iff (A^2Bx, 3ABy) \equiv (10, 6), (37, 33), (64, 60) \pmod{81}$$
$$a_{6,3} = 2 \pmod 3 \iff (A^2Bx, 3ABy) \equiv (10, 33), (37, 60), (64, 6) \pmod{81}$$

And finally, when $3ABy \equiv 15 \pmod{27}$, we have that

$$a_{6,3} = 0 \pmod 3 \iff (A^2Bx, 3ABy) \equiv (19, 42), (46, 69), (73, 15) \pmod{81}$$
$$a_{6,3} = 1 \pmod 3 \iff (A^2Bx, 3ABy) \equiv (19, 69), (46, 15), (73, 42) \pmod{81}$$
$$a_{6,3} = 2 \pmod 3 \iff (A^2Bx, 3ABy) \equiv (19, 15), (46, 42), (73, 69) \pmod{81}$$

Now let us take a look at $P \pmod 3$. When $(A^2Bx, 3ABy) \equiv (1, 78), (28, 24), (55, 51) \pmod{81}$, we have that $P \equiv X^3 + X^2 = X^2(X + 1) \pmod 3$, which has a double root $a = 0$ in $\mathbb{F}_3$. For $(A^2Bx, 3ABy) \equiv (1, 24), (28, 51), (55, 78) \pmod{81}$, we have that $P \equiv X^3 + X^2 + 1 = (X + 2)(X^2 + 2X + 2)$, which has simple roots over $\overline{\mathbb{F}}_3$. In the case $(A^2Bx, 3ABy) \equiv (1, 51), (28, 78), (55, 24) \pmod{81}$, our polynomial is of the form $P \equiv X^3 + X^2 + 2 \pmod 3$, that has simple roots over $\overline{\mathbb{F}}_3$. We have that $P \equiv X^3 + X^2 + X = X(X + 2)^2 \pmod 3$, that has a double root $a = 1$ over $\mathbb{F}_3$, when we are in the case

$(A^2Bx, 3ABy) \equiv (10, 60), (37, 6), (64, 33) \pmod{81}$. On the other hand $P \equiv X^3 + X^2 + X + 1 \equiv (X + 1)(X^2 + 1) \pmod 3$, which has simple roots over $\overline{\mathbb{F}}_3$, when $(A^2Bx, 3ABy) \equiv (10, 6), (37, 33), (64, 60) \pmod{81}$. The polynomial is of the form $P \equiv X^3 + X^2 + X + 2 \pmod 3$, which also has simple roots over $\overline{\mathbb{F}}_3$ when $(A^2Bx, 3ABy) \equiv (10, 33), (37, 60), (64, 6) \pmod{81}$. Now, we have that $P \equiv X^3 + X^2 + 2X \equiv X(X^2 + X + 2) \pmod 3$, with simple roots over $\overline{\mathbb{F}}_3$, when $(A^2Bx, 3ABy) \equiv (19, 42), (46, 69), (73, 15) \pmod{81}$. While for $(A^2Bx, 3ABy) \equiv (19, 69), (46, 15), (73, 42) \pmod{81}$, we see that $P \equiv X^2 + X^2 + 2X + 1 \pmod 3$, which turns out to have simple roots over $\overline{\mathbb{F}}_3$. And finally, when $(A^2Bx, 3ABy) \equiv (19, 15), (46, 42), (73, 69) \pmod{81}$, we have that $P \equiv X^3 + X^2 + 2X + 2 \equiv (X + 2)(X + 1)^2 \pmod 3$, which has a double root. Now looking to algorithm for the case $p = 3$, when it has a double root, we proceed after step 10, to step 16, where we find out that $f_3 = 2$, Tate's case 7 according to Papadopoulos' table. And as before when P has simple roots, $f = v - 4 \geq 2$. Using `MAGMA`, we see that for the cases where our polynomial P has simple roots we have that $v_3(Cz^n) = 3$, so we have that $v = 6$ and $f_3 = 2$, so we are in case Tate 6. When P has double roots we see that $v_3(Cz^n) \geq 7$ so $v \geq 7$. So we are done with case **IV**. We turn to case **V**

First of all, let us recall that in this case we have that $v_3(ABx) = 0$, and $A^2Bx \equiv 2 \pmod 3$, so $r_1 = 2$ and we have to change our coefficients. These are our new coefficients:

$$a_1 = 0, \quad a_2 = 6, \quad a_3 = 0, \quad a_4 = 3ABy + 12, \quad \text{and}$$
$$a_6 = 2A^2Bx + 6ABy + 8.$$

About the values of $v_3(c_4), v_3(c_6)$ and v, just in case **IV**, we have the following cases:

- If $3 \mid y$ then $v_3(c_4) \geq 3, v_3(c_6) = 3$ and $v = 3$.
- If $3 \mid Cz$ then $v_3(c_4) = 2, v_3(c_6) = 3$ and $v \geq 4$.
- If $3 \nmid Cyz$ then $v_3(c_4) = 2, v_3(c_6) = 3$ and $v = 3$.

We move on to the next step. In step 5 if $p^2 \nmid a_6$, then set $f_3 = v$ and we are finished. We have that $a_6 = 2A^2Bx + 6ABy + 8$, recall that we have also $3 \nmid ABx$ and $A^2Bx \equiv 12 \pmod 3$. If $3 \mid y$ then $9 \mid 6ABy$ and so, in order to have $9 \mid a_6$ we must have that $2A^2Bx + 8 \equiv 0 \pmod 9$, that is $A^2Bx \equiv 5 \pmod 9$. If $3 \nmid y$, then $A^2Bx \equiv 2, 5$ or $8 \pmod 9$. Consider first that $A^2Bx \equiv 2 \pmod 9$, then in order to have $a_6 \equiv 0 \pmod 9$ we must have $3ABy \equiv 3 \pmod 9$. Turning now to the case $A^2Bx \equiv 5 \pmod 9$ we get that $3ABy \equiv 0 \pmod 9$ in order to have $p^2 \mid a_6$, which implies that $3 \mid y$. And finally when we have $A^2Bx \equiv 8 \pmod 9$, if we have $a_6 \equiv 0 \pmod 9$ then we have that $3ABy \equiv 6 \pmod 9$. So when $(A^2Bx, 3ABy) \equiv (2,3), (5,0), (8,6) \pmod 9$, we have $p^2 \mid a_6$. On the other hand when we have $(A^2Bx, 3ABy) \equiv (2,0), (2,6), (5,3), (5,6), (8,0), (8,3) \pmod 9$ we have that $p^2 \nmid a_6$, so we have finished for these cases, with $f_3 = v$. By Papadopoulos we can be in case Tate 3 not P_2, with $f_3 = v = 3$ or in case Tate 4, with $f_3 = v = 4$. Using `MAGMA`, we see that when $(A^2Bx, 3ABy) \equiv (5,6), (2,6) \pmod 9$ then $v_3(Cz^n) = 1$, whille for the other cases $v_3(Cz^n) = 0$. So for $(A^2Bx, 3ABy) \equiv (2,6), (5,6) \pmod 9$ we are in Tate's case 4. For the remaining ones, to show that we are in case Tate 3 not P_2, we must see that there is no $r \in \mathbb{Z}$ such that

$$r^3 + b_2r^2 + 8b_4r + 16b_6 \equiv 0 \pmod{3^2}.$$

This is easily verified with a simple algorithm implemented on `MAGMA`. Also using `MAGMA` we see that when $(A^2Bx, 3ABy) \equiv (2,3), (5,0) \pmod 9$, $v_3(Cz^n) = 0$

implying that $v = 3$ and that when $(A^2Bx, 3ABy) \equiv (8, 6) \pmod 9$ then $v_3(Cz^n) \geq 2$, that is $v \geq 5$. We move now to step 6. If $p^3 \nmid b_8$, set $f_3 = v - 1$ and we are finished. We have that $b_8 = -9A^2B^2y^2 + 48A^2Bx + 72ABy + 48$. Now $p^3 \mid b_8 \iff (A^2Bx, 3ABy) \equiv (8, 6) \pmod 9$, and so for $(A^2Bx, 3ABy) \equiv (2, 3), (5, 0) \pmod 9$ we have finished with $f_3 = v - 1 = 2$, and so we are in case Tate 4 P_2. In fact, for these cases we have that the congruence $r^3 + b_2r^2 + 8b_4r + 16b_6 \equiv 0 \pmod 9$ has a solution for some $r \in \mathbb{Z}$. So we are still left with $(A^2Bx, 3ABy) \equiv (8, 6) \pmod 9$. Proceed then to step 7. If $p^3 \nmid b_6$ then set $f_3 = v - 2$ and we are finished. In this case we have $b_6 = 8A^2Bx + 24ABy + 32$. So $p^3 \mid b_6$ if and only if $(A^2Bx, 3ABy) \equiv (8, 15), (17, 6), (26, 24) \pmod{27}$. Therefore $p^3 \nmid b_6$ if and only if $(A^2Bx, 3ABy) \equiv (8, 6), (8, 24)(17, 15), (17, 24)(26, 6), (26, 15) \pmod{27}$, so for these case we are finished with $f_3 = v - 2 \geq 3$. By Tate's case 5, with $v = 5$ and $f_3 = 3$. In fact, using `MAGMA`, it's possible to see that for this cases we have $v_3(Cz^n) = 2$. For the remaining cases we move to step 8. If $p^3 \nmid a_6$, set $k \equiv a_3 \pmod 9$, but since $a_6 = 2A^2Bx + 6ABy + 8$, and we have that $b_6 = 4 * a_6$, so since $p^3 \mid b_6$ we have that $p^3 \mid a_6$. So we move to the next step. As before, we now have that $p \mid a_2, p^2 \mid a_4$ and $p^3 \mid a_6$. Set $P = X^3 + a_{2,1}X^2 + a_{4,2}X + a_{6,3}$. We clearly see that $a_{2,1} \equiv 2 \pmod 3$, and that $a_{4,2} \equiv 0, 1, 2 \pmod 3$ if $3ABy \equiv 15, 24, 6 \pmod{27}$ respectively. Now let us take a look at $P \pmod 3$. When $a_{4,2} \equiv 0$ and $a_{6,3} = 0$, we have that $P \equiv X^3 + 2X^2 = X^2(X + 2) \pmod 3$, which has a double root $a = 0$ in $\mathbb{F}_3$. For $a_{4,2} \equiv 0$ and $a_{6,3} = 1$,, we have that $P \equiv X^3 + 2X^2 + 1 \pmod 3$, which has simple roots over $\overline{\mathbb{F}}_3$. In the case $a_{4,2} \equiv 0$ and $a_{6,3} = 0$,, our polynomial is of the form $P \equiv X^3 + 2X^2 + 2 \equiv (X + 1)(X^2 + X + 2) \pmod 3$, that has simple roots over $\overline{\mathbb{F}}_3$. We have that $P \equiv X^3 + 2X^2 + X = X(X + 1)^2 \pmod 3$, that has a double root $a = 2$ over $\mathbb{F}_3$, when we are in the case $a_{4,2} \equiv 1$ and $a_{6,3} = 0$. On

the other hand $P \equiv X^3 + 2X^2 + X + 1 \pmod 3$, which has simple roots over $\overline{\mathbb{F}}_3$, when $a_{4,2} \equiv 1 \pmod 3$ and $a_{6,3} \equiv 1 \pmod 3$. The polynomial is of the form $P \equiv X^3+2X^2+X+2 \equiv (X+2)(X^2+1) \pmod 3$, which also has simple roots over $\overline{\mathbb{F}}_3$ when we have $a_{4,2} \equiv 1 \pmod 3$ and $a_{6,3} \equiv 2 \pmod 3$. Now, we have that $P \equiv X^3 + 2X^2 + 2X \equiv X(X^2 + 2X + 2) \pmod 3$, with simple roots over $\overline{\mathbb{F}}_3$, when $a_{4,2} \equiv 2 \pmod 3$ and $a_{6,3} = 0 \pmod 3$. While for $a_{4,2} \equiv 2 \pmod 3$ and $a_{6,3} = 1 \pmod 3$, we see that $P \equiv X^2 + 2X^2 + 2X + 1 = (X + 2)(X + 1)^2 \pmod 3$, which has a double root $a = 2$ in $\mathbb{F}_3$. And finally, when $a_{4,2} \equiv 2 \pmod 3$ and $a_{6,3} = 2 \pmod 3$, we have that $P \equiv X^3 + X^2 + 2X + 2 \pmod 3$, which has simple roots. Now using `MAGMA`, once again, we are able to which cases of $(A^2Bx, 3ABy) \pmod{81}$ correspond to each of the polynomials mentioned above. Here is the list, we start with the cases where $3ABy \equiv 15 \pmod{27}$, then

$$a_{6,3} = 0 \pmod 3 \iff (A^2Bx, 3ABy) \equiv (8, 69), (35, 42), (62, 15) \pmod{81}$$
$$a_{6,3} = 1 \pmod 3 \iff (A^2Bx, 3ABy) \equiv (8, 42), (35, 15), (62, 69) \pmod{81}$$
$$a_{6,3} = 2 \pmod 3 \iff (A^2Bx, 3ABy) \equiv (8, 15), (35, 69), (62, 42) \pmod{81}$$

When we have that $3ABy \equiv 24 \pmod{27}$, we have that

$$a_{6,3} = 0 \pmod 3 \iff (A^2Bx, 3ABy) \equiv (26, 51), (53, 24), (80, 78) \pmod{81}$$
$$a_{6,3} = 1 \pmod 3 \iff (A^2Bx, 3ABy) \equiv (26, 24), (53, 78), (80, 51) \pmod{81}$$
$$a_{6,3} = 2 \pmod 3 \iff (A^2Bx, 3ABy) \equiv (26, 78), (53, 51), (80, 24) \pmod{81}$$

And finally, when $3ABy \equiv 6 \pmod{27}$, we have that

$$a_{6,3} = 0 \pmod 3 \iff (A^2Bx, 3ABy) \equiv (17, 60), (44, 33), (71, 6) \pmod{81}$$
$$a_{6,3} = 1 \pmod 3 \iff (A^2Bx, 3ABy) \equiv (17, 33), (44, 6), (71, 60) \pmod{81}$$
$$a_{6,3} = 2 \pmod 3 \iff (A^2Bx, 3ABy) \equiv (17, 6), (44, 60), (71, 33) \pmod{81}$$

Same as in case **IV**, we have that by looking at the algorithm for the case $p = 3$, when it has a double root, we proceed after step 10, to step 16, where we find out that $f_3 = 2$, Tate's case 7 according to Papadopoulos' table. And as before when P has simple roots, $f = v - 4 \geq 2$. Using `MAGMA`, we see that for the cases where our polynomial P has simple roots we have that $v_3(Cz^n) = 3$, so we have that $v = 6$ and $f_3 = 2$, so we are in case Tate 6. When P has double roots we see that $v_3(Cz^n) \geq 7$ so $v \geq 7$. So we are done with case **V**.

5.2.4 Exponent for $p \geq 5$

Now we turn to the case when p is a prime greater or equal to 5. For that we apply Algorithm 5.1.1. Now we set $v = v_p(\Delta)$, so we have that

$$v = \begin{cases} 3v_p(A) & \text{if } 3 \mid ax, \\ 2v_p(B) & \text{if } 3 \mid By, \\ v_p(C) + nv_p(z) & \text{if } 3 \mid Cz, \\ 1 & \text{othwerise.} \end{cases} \tag{5.8}$$

We start our algorithm. First we compute $c_4 = -2^4 3^2 ABy$, $c_6 = -2^6 3^2 A^2 Bx$, $\Delta = -2^6 3^3 A^3 B^2 Cz^n$ and $j = 2^6 3^3 By^3 / Cz^n$. If $v_p(j) < 0$ set $k = v - v_p(j)$, else set $k = v$. Move on to the next step. In step 2 we re-arrange the equation to transform it in a minimal one. Is $k < 12$? If $v_p(j) < 0$ then $k = v_p(j) + v_p(\Delta) = -v_p(\Delta) + v_p(\Delta)$, since we only have $v_p(j) < 0$ if $p \mid Cz^n$. Otherwise $p \mid AB$ and due to our assumptions we have that $3v_p(A) \leq 3$ and $2v_p(B) \leq 4$, so we have that $k < 12$. Set $u \leftarrow 1, r \leftarrow 0, s \leftarrow 0$ and $t \leftarrow$. We proved to step 3. If $v_p(j) < 0$, that is when $p \mid Cz$, then set $v_1 = -v_p(j)$. So in this case we have that $v \geq 1$, $v_p(c_4) = v_p(c_6) = 0$. By Papadopoulos we have that we can only be in case Tate 2, with $v \geq 1$ and $f_p = 1$. k must be equal to 0 or 6. In this case we

have that $k = v_p(\Delta) + v_p(j) = v_p(C) + nv_p(z) - v_p(C) - nv_p(z) = 0 \pmod{12}$. So $f_p = 1$, as predicted by Papadopoulos. If $v_p(j) \geq 0$, that is $p \mid By$, $p \mid Ax$, or $p \nmid ABCxyz$ we move to step 4. Now if $p \mid Ax$ then $v_p(j) = 0$, $v = 3v_p(A) \geq 0$, $v_p(c_4) = v_p(A) \geq 0$ and $v_p(c_6) = 2v_p(A) + v_p(x) \geq 1$. If we have that $p \mid By$ then $v_p(j) \geq 1$, $v = 2v_p(B) \geq 0$, $v_p(c_4) = v_p(By) \geq 1$ and $v_p(v_6) = v_p(B) \geq 0$. When $p \nmid ABCxyz$ then $v_p(j) = v = v_p(c_4) = v_p(c_6) = 0$. Then first if $k = 0$ then $f_p = 0$, that is when $p \nmid ABCz$, case Tate 1, else $f_p = 2$, that is when $p \mid AB$, case Tate 3,4,5. So the conductor of our Frey curve $E_{(2,3,n)}$ is given by the following formula

$$N_{E_{(2,3,n)}} = 2^{f_2} 3^{f_3} \prod_{\substack{p \geq 5 \text{prime}, \\ p \mid ABCz}} p^{f_p}$$

where f_2, f_3 and f_p are given in the following tables, Table 5.7, Table 5.8 and Table 5.9. In Table 5.8 R_1 and R_2 stand for the following lists:

$$R_1 : \{(1,24),(1,51),(8,15),(8,42),(10,6),(10,33),(17,6),(17,60),(19,42),$$
$$(19,69),(26,24),(26,78),(28,51),(28,78),(35,15),(35,69),(37,33),(37,60),$$
$$(44,33),(44,60),(46,15),(46,69),(53,51),(53,78),(55,24),(55,78),(62,42),$$
$$(62,69),(64,6),(64,60),(71,6),(71,33)(73,15),(73,42),(80,24),(80,51)\},$$
$$R_2 : \{(1,78),(8,69),(10,60),(17,33),(19,15),(26,51),(28,24),(35,42),(37,6),$$
$$(44,6),(46,42),(53,24),(55,51),(62,15),(64,33),(44,6),(73,69),(80,78)\}.$$

With this we have completed the proof of Theorem 5.1

5.3 Final comments

We wanted to use this Frey curve and the possible levels for the newform to eliminate some exponents for the cases we are left with, especially the cases where

Table 5.7: Values of the exponent for the conductor with $p = 2$

$v_2(A)$	$v_2(x)$	$v_2(B)$	$v_2(y)$	$v_2(Cz^n)$	$(2A^2Bx, ABy) \equiv$	$(v_2(c_4), v_2(c_6), v^a)$	f_2	Tate's case
1	≥ 0	0	0	0		$(5, \geq 8, 9)$	$v - 1 = 8$	4
0	0	1	0	0		(5,7,8)	$v - 1 = 7$	4
0	0	1	1	0	$(4, 4), (4, 12) \pmod{16}$	$(6, 7, 8)$	$v - 5 = 3$	7^*
0	0	1	1	0	$(12, 4), (12, 12) \pmod{16}$	$(6, 7, 8)$	$v - 4 = 4$	6^*
0	0	1	≥ 2	0	$(4, 0), (4, 8) \pmod{16}$	$(\geq 7, 7, 8)$	$v - 6 = 2$	8^*
0	0	1	≥ 2	0	$(12, 0), (12, 8) \pmod{16}$	$(\geq 7, 7, 8)$	$v - 4 = 4$	6^*
0	0	2	≥ 0	0		$(\geq 6, 8, 10)$	$v - 4 = 6$	6
0	0	0	≥ 1	0		$(\geq 5, 6, 6)$	$v = 6$	3
0	0	0	0	1	$(2, 1) \pmod{4}$	$(4, 6, 7)$	$v = 7$	3
0	0	0	0	2	$(2, 3), (10, 11) \pmod{16}$	$(4, 6, 8)$	$v - 4 = 4$	6^*
0	0	0	0	2	$(2, 11), (10, 2) \pmod{16}$	$(4, 6, 8)$	$v - 5 = 3$	7^*
0	0	0	0	3	$(2, 7), (10, 15) \pmod{16}$	$(4, 6, 9)$	$v - 4 = 5$	6
0	0	0	0	4	$(2, 15), (10, 7), (18, 31), (26, 23) \pmod{32}$	$(4, 6, 10)$	$v - 6 = 4$	7^*
0	0	0	0	≥ 5	$(2, 31), (10, 23), (18, 31), (26, 7) \pmod{32}$	$(4, 6, \geq 11)$	4	7^*
0	0	0	0	2	$(6, 3), (14, 11) \pmod{16}$	$(4, 6, 8)$	$v - 4 = 4$	6^*
0	0	0	0	2	$(6, 11), (14, 3) \pmod{16}$	$(4, 6, 8)$	$v - 6 = 2$	8^*
0	0	0	0	3	$(6, 15), (14, 7) \pmod{16}$	$(4, 6, 9)$	$v - 4 = 5$	6
0	0	0	0	4	$(6, 23), (22, 7), (14, 31), (30, 15) \pmod{32}$	$(4, 6, 10)$	$v - 7 = 3$	9^*
0	0	0	0	5	$(14, 15), (30, 63), (46, 47), (62, 31)$ $(6, 7), (22, 55), (38, 39), (54, 23) \pmod{64}$	$(4, 6, 11)$	$v - 8 = 3$	10^*
0	0	0	0	6	$(14, 47), (30, 31), (46, 15), (62, 63)$ $(6, 39), (22, 23), (38, 7), (54, 55) \pmod{64}$	$(4, 6, 12)$	0	1
0	0	0	0	≥ 7	$(14, 47), (30, 31), (46, 15), (62, 63)$ $(6, 39), (22, 23), (38, 7), (54, 55) \pmod{64}$	$(4, 6, \geq 13)$	1	2
0	≥ 1	0	0	0	$(0, 1) \pmod{4}$	$(4, \geq 6, 6)$	$v - 1 = 5$	4^*
0	≥ 1	0	0	0	$(0, 3) \pmod{4}$	$(4, \geq 6, 6)$	$v = 6$	3^*

[a] $v := v_2(\Delta)$

Table 5.8: Values of the exponent for the conductor with $p = 3$

$v_3(A)$	$v_3(x)$	$v_3(B)$	$v_3(y)$	$v_3(Cz^n)$	$(A^2Bx, 3ABy) \equiv$	$(v_3(c_4), v_3(c_6), v^{a})$	f_2	Tate's case
1	0	0	0	0		$(3, 5, 6)$	$v - 2 = 4$	5
1	≥ 1	0	0	0		$(3, \geq 6, 6)$	$v - 4 = 2$	6
0	0	1	≥ 0	0		$(\geq 3, 4, 5)$	$v = 5$	3
0	0	2	≥ 0	0		$(\geq 4, 5, 7)$	$v - 2 = 5$	5
0	1	0	0	0		$(2, 4, 3)$	$v = 3$	3
0	1	0	0	0		$(2, \geq 5, 3)$	$v - 1 = 2$	4
0	0	0	≥ 1	0	$(1, 0), (2, 0), (7, 0), (8, 0) \pmod 9$	$(\geq 3, 3, 3)$	$v = 3$	3 not P_2
0	0	0	0	1	$(5, 6), (4, 6), (8, 6), (7, 6) \pmod 9$	$(2, 3, 4)$	$v = 4$	3
0	0	0	0	0	$(1, 3), (4, 3), (5, 3), (8, 3) \pmod 9$	$(2, 3, 3)$	$v = 3$	3 not P_2
0	0	0	≥ 1	0	$(4, 0), (5, 0) \pmod 9$	$(\geq 3, 3, 3)$	$v - 1 = 2$	4 P_2
0	0	0	0	0	$(2, 3), (7, 3) \pmod 9$	$(2, 3, 3)$	$v - 1 = 2$	4 P_2
0	0	0	0	2	$(1, 6), (1, 15), (8, 6), (8, 24), (10, 15), (10, 24), (17, 15), (17, 24), (19, 6), (19, 24), (26, 6), (26, 15) \pmod{27}$	$(2, 3, 5)$	$v - 2 = 3$	5
0	0	0	0	3	$R_1 \pmod{81}$	$(2, 3, 6)$	$v - 4 = 2$	6
0	0	0	0	≥ 4	$R_2 \pmod{81}$	$(2, 3, \geq 7)$	2	7

[a] $v := v_3(\Delta)$

Table 5.9: Values of the exponent for the conductor with $p \geq 5$

$v_p(A)$	$v_p(x)$	$v_p(B)$	$v_p(y)$	$v_p(Cz^n)$	$(v_{p,4}{}^a, v_{p,6}{}^b, v^c)$	$v_p(j)$	f_p	TC^d
0	0	0	0	≥ 1	$(0, 0, \geq 1)$	≤ -1	1	2
1	≥ 0	0	0	0	$(1, \geq 2, 3)$	0	2	4
0	≥ 1	0	0	0	$(0, \geq 1, 0)$	0	0	1
0	0	1	≥ 0	0	$(\geq 1, 1, 2)$	1	2	3
0	0	2	≥ 0	0	$(\geq 2, 2, 4)$	2	2	5
0	0	0	≥ 1	0	$(\geq 1, 0, 0)$	≥ 3	0	1

[a] $v_p(c_4)$
[b] $v_p(c_6)$
[c] $v := v_p(\Delta)$
[d] Tate's Case

Table 5.10: Possible values for N_p

D	N_p
33	$2^{\alpha_2} \times 3^5 \times 11^2$
41	$2^{\alpha_2} \times 3^{\alpha_3} \times 41^2$
57	$2^{\alpha_2} \times 3^5 \times 19^2$
68	$2^6 \times 3^{\beta_3} \times 17^2$
73	$2^{\alpha_2} \times 3^{\beta_3} \times 73^2$
90	$2^7 \times 3^5 \times 5^2$
97	$2^{\alpha_2} \times 3^{\beta_3} \times 97^2$
98	$2^7 \times 3^{\alpha_3} \times 7^2$

D is not a square plus or minus one. But unfortunately nowadays there is not enough computational power to calculate the newforms and eliminated them using the level lowering method (Method I). The reason for this is the high level for the possible newforms, we present a table with the possible values of N_p for each case of D still left to eliminate, and where we think there are no integral solutions.

Hopefully in a nearby future, there will be enough computational power to calculate the newforms pretended as well use the Methods exposed in Chapter 3 to help us find all the solutions for the values of D given in the Table 5.10.

Appendix A

Tables with the final results

Table A.1: Solutions for $x^2 + D = y^n$ with D in the range (R) and $n \geq 2$ and that are completely solved

D	Solutions $(\|x\|, y, n)$
-1	$(1, 0, n), (0, -1, n)$ with n odd , $(3, 2, 3)$
-4	$(2, 0, n), (6, 2, 5)$
-6	
-7	$(4, \pm 3, 2)$
-9	$(3, 0, n), (5, \pm 4, 2), (5, \pm 2, 4), (15, 6, 3), (1, -2, 3), (253, 40, 3), (6, 3, 3)$
-11	$(6, \pm 5, 2), (56, 5, 5)$
-12	$(4, \pm 2, 2), (2, -2, 3), (47, 1 \pm 3, 2)$
-13	$(7, \pm 6, 2), (16, 3, 5)$
-14	
-16	$(4, 0, n), (5, \pm 3, 2), (12, 2, 7)$
-18	$(19, 7, 3)$
-19	$(10, \pm 9, 2), (12, 5, 3)$
-20	$(6, \pm 4, 2), (6, \pm 2, 4)$
-21	$(5, \pm 2, 2), (11, \pm 10, 2)$
-22	$(7, 3, 3), (47, 3, 7)$
-23	$(12, \pm 11, 2)$
-25	$(5, 0, n), (13, \pm 12, 2),$
-27	$(6, 3, 2), (14, \pm 13, 2), (0, -3, 3)$
-28	$(8, \pm 6, 2), (1, -3, 3), (6, 2, 3)$

-29	$(15, \pm 14, 2)$
-30	$(83, 19, 3)$
-31	$(16, \pm 15, 2), (2, -3, 3)$
-32	$(9, \pm 7, 2), (6, \pm 2, 2), (8, 2, 5), (0, -2, 5)$
-34	
-36	$(6, 0, n), (10, \pm 8, 2), (3, -3, 3), (10, 4, 3), (42, 12, 3), (2, -2, 5)(10, \pm 2, 6)$
-38	$(37, 11, 3)$
-39	$(8, \pm 5, 2), (20, \pm 19, 2)$
-40	$(11, \pm 9, 2), (7, \pm 3, 2), (16, 6, 3), (11, \pm 3, 4)$
-42	
-43	$(22, \pm 21, 2), (4, -3, 3)$
-44	$(12, \pm 10, 2), (6, -2, 3), (13, 5, 3)$
-45	$(7, \pm 2, 2), (9, \pm 6, 2), (23, \pm 22, 2)$
-46	$(17, 3, 5)$
-47	$(24, \pm 23, 2)$
-49	$(7, 0, n), (25, \pm 24, 2), (9, 2, 5)$
-51	$(10, \pm 7, 2), (26, \pm 25, 2), (26, \pm 5, 4)$
-52	$(14, \pm 12, 2), (5, -3, 3)$
-53	$(27, \pm 26, 2)$
-54	$(9, 3, 3)$
-55	$(8, \pm 3, 2), (28, \pm 27, 2), (28, 9, 3), (28, \pm 3, 6)$
-56	$(9, \pm 5, 2), (15, \pm 13, 2), (8, 2, 3)$
-58	
-59	$(30, \pm 29, 2)$
-60	$(8, \pm 2, 2), (16, \pm 14, 2)$
-61	$(31, \pm 30, 2)$
-62	
-64	$(8, 0, n), (10, \pm 6, 2), (1, \pm 15, 2), (0, -4, 3), (24, 8, 3), (24, 2, 9)$
-66	
-67	$(34, \pm 33, 2)$
-69	$(13, \pm 10, 2), (35, \pm 34, 2),$
-70	
-71	$(36, \pm 35, 2), (14, 5, 3),$
-72	$(9, \pm 3, 2), (11, \pm 7, 2), (19, \pm 17, 2), (8, -2, 3)$
-74	

-75	$(10, \pm 5, 2), (14, \pm 11, 2), (38, \pm 37, 2)$
-76	$(20, \pm 18, 2), (7, -3, 3),$
-77	$(9, \pm 2, 2), (39, \pm 38, 2)$
-78	
-79	$(40, \pm 39, 2), (302, 45, 3)$
-81	$(9, 0, n), (41, \pm 40, 2), (7, -2, 5), (18, 3, 5)$
-83	$(42, \pm 41, 2)$
-84	$(10, \pm 4, 2), (22, \pm 20, 2)(10, \pm 2, 4)$
-85	$(11, \pm 6, 2), (43, \pm 42, 2)$
-86	
-87	$(16, \pm 13, 2), (44, \pm 43, 2),$
-88	$(13, \pm 9, 2), (23, \pm 21, 2), (13, \pm 3, 4)$
-89	$(45, \pm 44, 2), (5, \pm 4, 3), (9, -2, 3), (33, 10, 3), (408, 55, 3), (11, 2, 5)$
-91	$(10, \pm 3, 2), (46, \pm 45, 2), (8, -3, 3)$
-92	$(24, \pm 22, 2), (10, 2, 3)$
-93	$(17, \pm 14, 2), (47, \pm 46, 2), (130, 7, 5)$
-94	$(11, 3, 3), (421, 3, 11)$
-95	$(12, \pm 7, 2), (48, \pm 47, 2)$
-96	$(10, \pm 2, 2), (11, \pm 5, 2), (14, \pm 10, 2), (25, \pm 23, 2), (8, -2, 5)$
-100	$(10, 0, n), (26, \pm 24, 2), (6, -4, 3), (15, 5, 3), (90, 20, 3), (118, 24, 3),$ $(137190, 2660, 3)$

Table A.2: Solutions for $x^2 + D = y^n$ with D in the range (**R**) and $n \geq 2$ and that are not completely solved

D	Solutions $(\|x\|, y, n)$
-2	$(1, -1, n)$, with n odd
-3	$(2, 1, n)$
-5	$(2, -1, n)$, with n odd, $(3, 2, 2)$
-8	$(3, 1, n), (4, 2, 3), (312, 46, 3), (0, -2, 3)$
-10	$(3, -1, n)$ with n odd,
-15	$(4, 1, n), (8, \pm 7, 2), (1138, 109, 3),$
-17	$(4, -1, n)$, with n odd,$(9, \pm 8, 2), (9, 4, 3), (3, 2, 3), (5, 2, 3), (23, 8, 3),$ $(282, 43, 3), (375, 52, 3), (378661, 5234, 3), (9, 2, 6)$
-24	$(5, 1, n), (7, \pm 5, 2), (4, -2, 3), (32, 10, 3), (736844, 8158, 3)$
-26	$(5, -1, n)$ with n odd, $(2537, 23, 5)$
-33	$(7, \pm 4, 2), (17, \pm 16, 2), (7, \pm 2, 4), (17, \pm 4, 4), (17, \pm 2, 8), (5, -2, 3), (1, -2, 5)$
-35	$(6, 1, n), (18, \pm 17, 2)$
-37	$(6, -1, n)$ with n odd, $(19, \pm 18, 2), (8, 3, 3), (3788, 243, 3), (3788, 27, 5)$ $(3788, 3, 15)$
-41	$(21, \pm 20, 2), (7, 2, 3), (3, -2, 5), (13, 2, 7)$
-48	$(7, 1, n), (8, \pm 4, 2), (13, \pm 11, 2), (8, \pm 2, 4), (4, -2, 5)$
-50	$(7, -1, n)$ with n odd,
-57	$(11, \pm 8, 2), (29, \pm 28, 2), (5, -2, 5), (7, -2, 3), (11, 4, 3), (20, 7, 3), (11, \pm 2, 6)$
-63	$(8, 1, n), (12, \pm 9, 2), (32, \pm 31, 2), (6, -3, 3), (12, \pm 3, 4)$
-65	$(8, -1, n)$ with n odd, $(9, \pm 4, 2), (33, \pm 32, 2), (1, -4, 3), (14113, 584, 3),$ $(9, \pm 2, 4), (33, 4, 5), (33, \pm 2, 10)$
-68	$(18, \pm 16, 2), (2, -4, 3), (1874, 152, 3), (18, \pm 4, 4), (14, 2, 7), (18, \pm 2, 8),$ $(4, -2, 11)$
-73	$(37, \pm 36, 2), (3, -4, 3), (9, 2, 3), (10, 3, 3), (17, 6, 3), (611, 72, 3), (6717, 356, 3),$ $(37, \pm 6, 4)$
-80	$(9, 1, n), (12, \pm 8, 2), (21, \pm 19, 2), (4, -4, 3), (12, 4, 3), (292, 44, 3), (12, \pm 2, 6)$
-82	$(8, -1, n)$ with n odd,
-90	
-97	$(49, \pm 48, 2), (15, 2, 7)$
-98	$(21, 7, 3),$
-99	$(10, 1, n), (18, \pm 15, 2), (50, \pm 49, 2), (50, \pm 7, 4)$

Appendix B

Magma code

In this appendix we give implementations for MAGMA of our algorithms to solve (**LN**). Note that sometimes the symbols used in the programs are different than those used in the main text.

B.1 Algorithm to compute the solutions of the equation $x^2 + D = y^2$

In this section we implement the algorithm described in section 2.2.4 to find all the solutions of $x^2 + D = y^2$, with $-100 \leq D \leq 100$ and $D \neq 0$.

```
for D in [-100..-1] cat [1..100] do
S:={};
for d in Divisors(Abs(D)) do
a:=(D div d)+d;
if IsEven(a) then
S:=S join { [a div 2,(a-2*d) div 2],[-a div 2,(a-2*d) div 2]};
end if;
end for;
printf "the solutions of the equation x^2-1*%o=y^2, are the following
```

```
        \n [x,y]:=%o\n", D, S;
end for;
```

B.2 Algorithm to compute the solutions of the equation $x^2 + D = y^3$

As we have said in section 2.5.1, MAGMA has a method already implemented to find integral points on a elliptic curve. So we use that function in order to find all the solutions of $x^2 + D = y^3$. The algorithm is the following.

```
for D in [-100..-1] cat [1..100] do
E:=EllipticCurve([0,D]);
IntPts:=IntegralPoints(E);
S:={[P[2],P[1]]:P in IntPts};
printf "the solutions of the equation x^2-1*%o=y^3, are the following
        \n [x,y]:=%o\n", D, S;
end for;
```

B.3 Code for Thue equations method

In this section we will present all the functions needed to solve the equation 2.2 using Thue equations as described in section 2.2.

B.3.1 Basic arithmetic function

We start by defining a function `Primefactors`, where given a number n as input we have as output the set of the prime factors of n, when $n = 0$ or 1, then the output is the empty set. This function we will also be needed in section B.4.

```
Primefactors:=function(n)
if n eq 0 or Abs(n) eq 1 then
return {};
end if;
if Abs(n) gt 1 then
return {p:p in PrimeBasis(n)};
end if;
end function;
```

B.3.2 The set Λ_n

We build this easy function to obtain the set Λ_n given in section 2.2.3.

```
UniSet:=function(Q,n)
if Discriminant(Q) lt 0 then
G,m:=UnitGroup(Q);
Gn:=sub<G|[n*G.i: i in [1..Ngens(G)]]>;
q,mq:=quo<G|Gn>;
return [(g@@mq   @m): g in q];
else
u:=FundamentalUnit(Q);
if n eq 2 then
return ([u^k: k in [0,1]] cat [-1*u^k: k in [0,1]]);
else
return [u^k: k in [0..n-1]];
end if;
end if;
end function;
```

B.3.3 The Selmer Group and Γ set

The functions presented in this section are related with the construction of the n-Selmer group of a number field $\mathbb{K}$ for a given finite set of prime ideals S.

We start by presenting a function that obtains the factorization of an ideal in an S-ideal times an ideal coprime with S given by Proposition 2.3.1.

```
SnIdealFactorization:=function(a,S,n)
F:=Factorization(a);
O:=Ring(Universe(S));
aSL:=[x : x in F| x[1] in S] cat [<1*O,1>];
aSPL:=[x: x in F| x[1] notin S and x[2] mod(n) eq 0] ;
aSPL:= aSPL cat [<1*O,1>];
aS:=&*[x[1]^x[2]: x in aSL];
aCS:=&*[x[1]^(x[2] div n):x in aSPL];
return aS*aCS eq a, aS, aCS;
end function;
```

The following function outputs an Abelian group G isomorphic to the n-Selmer group ouf $\mathbb{K}$ for given finite set of prime ideals S, as an homomorphism m from $\mathbb{K}^*$ to the abelian group G, that comutes with the natural projection of $\mathbb{K}$ on the n-Selmer group and the isomorphism between the n-Selmer group and the group G.

```
nSelmerGroup:=function(n,S)
O:=Ring(Universe(S));K:=NumberField(O);
C, mC:= ClassGroup(O);
Cn:= sub <C|[n*C.i: i in [1..Ngens(C)]]>;
q,mq:= quo <C|Cn>;
SS:= {Parent(1*O)|};
s:= sub <q| [x@@mC @ mq : x in S]>;
p_Z:=2;
while s ne q do
```

```
lp:=Factorization(p_Z*O);
lp:= [x[1] : x in lp | Norm(x[1]) le 10^3 or Degree(x[1]) eq 1];
for i in lp do
if i in S then
continue;
end if;
I :=i@@mC@mq;
if not I in S then
Include(~SS, i);
s:= sub<q|s, I>;
end if;
end for;
p_Z:= NextPrime(p_Z);
end while;
U, mU, bU:= SUnitGroup([Universe(S)|x:x in S join SS]:Raw);
SbU:=[x[1]:x in Factorization((&*Eltseq(bU))*O)];
mbU:=Matrix([[Valuation(x,y):y in SbU]: x in Eltseq(bU)]);
sL:=Setseq(S join SS);
m1:=Matrix([Eltseq(x@@mC): x in sL]);
if #SS eq 0 then
k:= U;
else
pG:=AbelianGroup([n: x in SS]);
vbU:= Matrix([[Valuation(x,y): y in SS]: x in Eltseq(bU)]);
h:= hom<U ->pG| [pG!Eltseq((U.i@mU)*vbU): i in [1..Ngens(U)]]>;
k:= Kernel(h);
end if;
KpS, mKpS := quo<k| [n*k.i: i in [1..Ngens(k)]]>;
SeIn:=KpS;
from_KpS := map<KpS -> NumberField(O) |
        x:-> PowerProduct(bU, x @@ mKpS @ mU)>;
to_KpS:=function(x)
```

```
if Parent(x) ne K then
error "error: Argument must be an element of", K;
end if;
if x eq 0 then
error "error: element should be non-zero";
end if;
st, aS, bS:=SnIdealFactorization(x*O,S,n);
if st then
m2:=Matrix([Eltseq(-(bS@@mC))]);
st,c:=IsConsistent(m1,m2);
if st then
J:=&*[sL[i]^c[1,i]: i in [1..#sL]];
_,elt:=IsPrincipal(J*bS);
xU:=K!(x*elt^(-n));
mxU:=Matrix([[Valuation(xU,y):y in SbU]]);
st, c2:=IsConsistent(mbU,mxU);
g:=U!(&+[c2[1,i]*U.i:i in [1..Ngens(U)]]);
return mKpS(k!g);
else
error
"error: the large set of Ideals does not generate C/pC";
end if;
else
error "error: element should be an algebraic number
which valuation modulo any prime ideal outside of S
is congruent to 0 mod %o",n;
end if;
end function;
return KpS, map<FieldOfFractions(O)->KpS|
                        x:->to_KpS(x),y:->from_KpS(y)>;
end function;
```

The following functions help to obtain the Γ' set from the n-Selmer Group as is presented in Theorem 2.4.

```
nPowerTest:=function(g,C,SC,n);
Ng:=Norm(g);
Ng2n:=&*[p^(Valuation(Ng,p) mod 2*n): p in SC];
C2n:=&*[p^(Valuation(C^2,p) mod 2*n): p in SC];
st:= Ng2n eq C2n;
return st;
end function;

smallSelmer:=function(p,D,C,IC,S);
S2D:=[p:p in PrimeDivisors(2*D)| p notin PrimeDivisors(C)];
SC:=[p:p in PrimeDivisors(C)];
SCF:=Factorization(C);
G,phi:=nSelmerGroup(p,S);
A:=FreeAbelianGroup(1);
Ap,psi:=quo<A|p*A>;
A2p,psi2:=quo<A|2*p*A>;
Gnew:=G;
for q in S2D do
h:=hom<Gnew->Ap | x :-> (Valuation(Norm(x@@phi),q)*A.1)@psi >;
Gnew:=Kernel(h);
end for;
Gnew:={g: g in Gnew};
for v in SCF do
Gnew:={g: g in Gnew | ((Valuation(Norm(g@@phi),v[1]) mod 2*p)
         eq (v[2] mod 2*p))};
end for;
return Gnew,G,phi;
end function;

SubsetTest:=function(IFA,g)
for Ip in IFA do
```

```
if Min([Valuation(g,Place(Ip[1])),
          Valuation(Conjugate(g),Place(Ip[1]))]) gt Ip[2] then
return false;
end if;
end for;
return true;
end function;

IExp:=function(m,n)
if m ge 0 then
return m;
else
return (m mod n);
end if;
end function;

TestIGCD:=function(I,IA)
J:=GCD(I,Conjugate(I));
for P in Factorization(J) do
if P[2] gt Valuation(IA, P[1]) then
return false;
end if;
end for;
return true;
end function;

SieveGCD:=function(Gnew,phi,IF2DC,O,n,I2DC,IF2D)
SetIp:={};
SetI1:={};
Ip2DC:={Ip[1]:Ip in IF2DC};
for g in Gnew do
I2DC:={@ Ip: Ip in Factorization((g@@phi)*O)| Ip[1] in Ip2DC @};
if #I2DC gt 0 then
```

```
NewI:=&*[Ip[1]^IExp(Ip[2],n):Ip in I2DC];
else
NewI:=1*O;
end if;
if  (NewI in (SetI1 join {Conjugate(I): I in SetI1})) eq false
        and SubsetTest(IF2D,NewI)  then
SetIp:=SetIp join {[NewI,(g@@phi)*O]};
SetI1:=SetI1 join {NewI};
end if;
end for;
return SetIp;
end function;
```

The following functions help to sieve the set Γ as is presented in Proposition 2.3.5.

```
LocInt:=function(G,I,a)
Q:=Parent(a);
O:=MaximalOrder(Q);
IL:=I*O;
LF:=Factorization(IL);
L1:=LF[1][1];
L2:=LF[2][1];
PL1:=Place(L1);
PL2:=Place(L2);
for g in G do
if (Valuation(g,L1) lt 0) or (Valuation(g,L2) lt 0) then
return false, L1, L2;
end if;
end for;
return true, L1,L2;
end function;

tlTest:=function(I,p,D,a,g,q,L1,L2)
```

```
n:=(l-1) div p;
F1, th1:=ResidueClassField(L1);
F2, th2:=ResidueClassField(L2);
i:=0;
repeat
t1:=(i-q*th1(a))^n;
t2:=(i-q*th2(a))^n;
r1:=(th1(g))^n;
r2:=(th2(g))^n;
if ((t1 eq r1) or (t1 eq 0)) and ((t2 eq r2) or (t2 eq 0)) then
return true;
else
i:=i+1;
end if;
until i eq l;
return false;
end function;


Gammapfunction:=function(p,D,d,q,GS,a)
S:={};
GR:={};
B:=1000;
l:=1;
repeat
repeat
repeat
repeat
repeat
repeat
l:=l+2*p;
if l gt (p*B+1) then
return GS;
end if;
```

```
until IsPrime(l);
until   (D mod l) eq 0 ;
until (KroneckerSymbol(d,l) eq 1);
st,L1,L2:=(LocInt(GS,l,a));
until st;
G1:={g: g in GS|tlTest(l,p,D,a,g,q,L1,L2)};
if #G1 lt #GS then
GS:=G1;
S:=Append(S,l);
end if;
until #GS eq 0;
return GS;
end function;
```

B.3.4 Building up the Thue equations from the set Γ

The next function constructs Thue equations from the set Γ as is stated in Theorem 2.1.

```
GamTHEqtns:=function(a,DW,n,GS,P,P1,Pt,Pt1)
Q:=Parent(a);
O:=MaximalOrder(Q);
GTE:={@@};
for g in GS do
ng:=Denominator(g);
intg:=O!(ng*g);
intgc:=Conjugate(intg);
fq:=(P*intg-P1*intgc)*DW/(2*a);
fx:=(P*intg+P1*intgc)*DW/2;
if Degree(Evaluate(fq,Pt)) eq n then
GTE:=GTE join
{@[Evaluate(fq,Pt),Evaluate(fx,Pt),ng, Integers()!Norm(g)]@};
```

```
end if;
if (Degree(Evaluate(fq,Pt)) lt n) and
   (Degree(Evaluate(fq,Pt1)) eq n) then
GTE:=GTE join
{@[Evaluate(fq,Pt1),Evaluate(fx,Pt1),ng, Integers()!Norm(g)]@};
end if;
end for;
return GTE;
end function;
```

B.3.5 Elimination methods for Thue equations

The following functions are used to implement the first elimination method, see section 2.4.1.

```
CoefDiv:=function(f);
d:=Degree(f);
Coef:=[];
for i in [1..d+1] do
Coef:=Coef cat [Coefficient(f,i-1)];
end for;
c:=GreatestCommonDivisor(Coef);
return c;
end function;

CoefTeste:=function(tp,q)
return IsDivisibleBy(q*tp[3],CoefDiv(tp[1]));
end function;
```

The following functions are used to implement the second elimination method, using local solvability, as it was presented in section 2.4.2.

```
Roots2Var:=function(f,p,v,q)
C:=GCD(CoefDiv(f),q);
```

```
m:=v+1;
n:=Degree(f);
if v eq 0 then
if IsDivisibleBy(C,p) then
return true;
else
Zp<x>:=PolynomialRing(GF(p));
for a in [0..p-1] do
F:=&+[Coefficient(f,i)*x^i*a^(n-i): i in [0..n]]-q;
if F eq 0 then
return true;
else
if #Roots(F) gt 0 then
return true;
end if;
end if;
end for;
return false;
end if;
else
v:=Valuation(C,p);
m1:=v+1;
S:=[[i,j]:i,j in [0..p^m1-1]];
while (#S gt 0) and (m1 le m)  do
S1:=[];
for P in S do
u:=P[1];
v:=P[2];
rest:=&+[Coefficient(f,i)*u^i*v^(n-i):i in [0..n]]-q;
if (rest mod p^m1) eq 0 then
S1:=S1 cat [P];
end if;
```

```
end for;
if #S1 eq 0 then
return false;
else
S:=[[P[1]+i*p^m1,P[2]+j*p^m1]: P in S1, i in [0..p-1],
         j in [0..p-1]];
m1:=m1+1;
end if;
end while;
return true;
end if;
end function;


LocalThueEquation:=function(th, q)
ng:=Integers()!(th[3]);
f:=th[1];
Discf:=Discriminant(f);
n:=Degree(f);
Zx:=Parent(f);
x:=Zx.1;
Z2uv<u,v>:=PolynomialRing(Integers(),2);
A<u1,v1>:=AffineSpace(Rationals(),2);
F:=&+[(Integers()!Coefficient(f,i))*u^i*v^(n-i):i in [0..n]]-q*ng;
genF:=(n+1)*(n+2)/2;
BndF:=
Truncate(n+2*genF^2-1+2*Sqrt(genF^4+(n-1)*genF^2))+1;
PrimeList1:={p: p in [1..BndF]|IsPrime(p)} join
        Primefactors(Discf) join Primefactors(n*ng);
DiscF1:=Integers()!Discriminant(Evaluate(F,[u,1]),u);
DiscF2:=Integers()!Discriminant(Evaluate(F,[1,v]),v);
if DiscF1*DiscF2 eq 0 then
BadPrimesF:=Primefactors(DiscF1+DiscF2)
```

```
        join PrimeList1;
else
BadPrimesF:=Primefactors(GCD(DiscF1,DiscF2))
        join PrimeList1;
end if;
for p in BadPrimesF do
v:=Valuation(n*q*ng,p);
if Roots2Var(f,p,v,q*ng) eq false then
return false;
end if;
end for;
return true;
end function;
```

This function is used to implement the third elimination method as we have presented in section 2.4.3.

```
Roots21Var:=function(f,p,v,q)
m:=v; n:=Degree(f);
if m eq 1 then
Zp<x>:=PolynomialRing(GF(p));
for a in [0..p-1] do
F:=&+[Coefficient(f,i)*x^i*a^(n-i): i in [0..n]]-q;
if F eq 0 then
return true;
else
if F ne 0 and #Roots(F) gt 0 then
return true;
end if;
end if;
end for;
return false;
else
```

```
A<u1,v1>:=AffineSpace(Integers(p^m),2);
C:=Curve(A,
  &+[Coefficient(f,i)*u1^i*v1^(n-i):i in [0..n]]-q);
i:=0;
while i lt p^m do
j:=0;
while j lt p^m do
P1:=A![i,j];
if (P1 in C) then
return true;
end if;
j:=j+1;
end while;
i:=i+1;
end while;
return false;
end if;
end function;


xFinThueEquations:=function(tp,D1,D2,D3,n)
GD13:=GCD(D2,D3);
if (Abs(D1) eq 1) and (GD13 eq 1) then
return true;
else
tx:=tp[2];
Z2uv<u,v>:=PolynomialRing(Integers(),2);
PD1:=Factorization(D1);
PD23:=[p: p in PrimeDivisors(GD13)|
        p notin PrimeDivisors(D1)];
for p in PD1 do
v:=p[2];p1:=p[1];
st:=Roots21Var(tx,p1,v,0);
```

```
if st eq false then
return false;
end if;
end for;
for p in PD23 do
v:=1;
st:=Roots21Var(tx,p,v,0);
if st eq false then
return false;
end if;
end for;
end if;
return true;
end function;
```

B.3.6 Solving Thue equations

The following functions are used to compute the solutions of a Thue equation. The first one help us to minimize the coefficients of a Thue equation (see page 47).

```
MinimizeThueCoef:=function(f,n,q)
Zuv<u,v>:=PolynomialRing(Integers(),2);
s:=Min([Abs(Coefficient(f,i)):i in [0..n]]);
f:=&+[Coefficient(f,i)*u^i*v^(n-i):i in [0..n]];
f1:=f;
S:=[1,0];
r:=s-1;
s1:=s;
A:=Matrix(Integers(),2,2, [1,0, 0,1]);
A1:=A;
while (r lt s) and (r ge 1) do
```

```
A:=A1;
s:=s1;
f:=f1;
r1:=r;
for a,b in [-3*10^3..3*10^3] do
if GCD(a,b) eq 1 then
s2:=Evaluate(f,[a,b]);
if (Abs(s2) gt 0) and (Abs(s2) lt r1) then
r1:=Abs(s2);
S:=[a,b];
end if;
if Abs(s2) eq q then
if s2 eq q then
S:=[a,b];
else
S:=[-1*a,-1*b];
end if;
break; break;
end if;
end if;
if r1 eq 1 then
break;
end if;
end for;
r:=Evaluate(f,S);
if r lt 0 then
S:=[-S[1],-S[2]];
r:=-1*r;
end if;
g,PL:=XGCD(S);
f1:=Evaluate(f,[S[1]*u-PL[2]*v,S[2]*u+PL[1]*v]);
fu:=Evaluate(f1,[u,1]);
```

```
s1:=Min([Coefficient(fu,u,i):i in [0..n]]);
B:=Matrix(Integers(),2,2, [S[1],-PL[2], S[2],PL[1]]);
A1:=A*B;
if r1 eq 1 then
A:=A1;
f:=f1;
end if;
end while;
return A,f;
end function;
```

This function help us to solve a Thue equation using the unimodular method as described in page 47, when it is possible or just using the methods already implemented in MAGMA to solve a Thue equation.

```
UnimodularThue:=function(n,tp,q1)
f:=tp[1];
q:=Integers()!(tp[3]*q1);
Zx:=Parent(f);
x:=Zx.1;
cn:=Abs(Coefficient(f,n));
c0:=Abs(Coefficient(f,0));
cGCD:=CoefDiv(f);
if (c0 lt cn) and (c0 gt 0) then
f:=Zx!(&+[(Coefficient(f,i) div cGCD)*x^(n-i): i in [0..n]]);
U1:=-1;
q1:= q div cGCD;
lcoef:=c0 div cGCD;
else
f:=Zx!(&+[(Coefficient(f,i) div cGCD)*x^(i): i in [0..n]]);
U1:=1;
q1:= q div cGCD;
lcoef:=cn div cGCD;
```

```
end if;
if lcoef eq 1 then
a:=1;
b:=0;
c:=0;
d:=1;
S:=Solutions(Thue(f),q1);
return S, U1, a, b, c, d;
else
if lcoef gt 1 then
A,f1:=MinimizeThueCoef(f,n,q);
f:=Evaluate(f1,[x,1]);
a:=A[1,1];
b:=A[1,2];
c:=A[2,1];
d:=A[2,2];
else
a:=1;
b:=0;
c:=0;
d:=1;
end if;
t:=Thue(f);
S1:=Solutions(t,1);
if #S1 eq 0 then
if q1 eq 1 then
S:=[];
return S, U1, a, b, c, d;
else
S:=Solutions(t,q1);
return S, U1, a, b, c, d;
end if;
```

```
else
if q1 eq 1 then
S:=S1;
return S, U1, a, b, c, d;
else
a1:=S1[1][1];
c1:=S1[1][2];
m,d1,b1:=XGCD(a1,c1);
g:=&+[Coefficient(f,i)*((a1*x-b1)^i)*((c1*x+d1)^(n-i)) :
        i in [0..n]];
S:=Solutions(Thue(g),q1);
a2:=a*a1+b*c1;
b2:=-a*b1+b*d1;
c2:=c*a1+d*c1;
d2:=-c*b1+d*d1;
return S,U1,a2,b2,c2,d2;
end if;
end if;
end if;
end function;
```

This function help us to determine if there was a solution of our equation 2.2 associated to a given a Thue equation.

```
ThueEqtsMethods:=function(tp,q1,D,C,DW)
n:=Degree(tp[1]);
SolutionSet:={};
PartialSol:={};;
S,U1,a,b,c,d:=UnimodularThue(n,tp,q1);
if #S eq 0 then
return SolutionSet;
else
for Sp in S do
```

```
NewS:=[a*Sp[1]+b*Sp[2],c*Sp[1]+d*Sp[2]];
if U1 eq 1 then
PartialSol := PartialSol join  {NewS, [-1*NewS[1],-1*NewS[2]]};
else
PartialSol:=PartialSol join {[NewS[2],NewS[1]],
        [-1*NewS[2],-1*NewS[1]]};
end if;
end for;
end if;
Xt:={&+[Coefficient(tp[2],i)*(Xs[1])^i*(Xs[2])^(n-i):i in [0..n]]:
        Xs in PartialSol};
ng:=Integers()!(tp[3]);
X:={Integers()!(x div (DW*ng)):  x in Xt|
        Root(((x/(DW*ng))^2+D)/C,n) in Integers()};
SolutionSet:={[x,Integers()!(Root((x^2+D)/C,n))]: x in X};
return SolutionSet;
end function;
```

B.3.7 The algortihm

Finally we give the algorithm to obtain the solutions of (2.2) for a given n (we present the algorithm for $n = 5$). We separate the algortihm in two parts, first deals with the case when $\mathbb{K}_D$ is a quadratic field, the second one when $\mathbb{K} = \mathbb{Q}$, following in this case the method presented in section 2.2.2.

```
Z:=Integers();
Z1<x>:=PolynomialRing(Z);
for D1 in [1..100] do
for D2 in [-100..100], D3 in [1..100] do
n:=5;
if (D2 ne 0)  then
D:=D1*D2;C:=D1*D3;D23:=GCD(D2,D3);
```

```
printf "The equation %o*x^2+1*%o=%o*y^%o,\n",
        D1,D2,D3,n;
d,q:=SquarefreeFactorization(D);
if -d ne 1 then
Q<a>:=QuadraticField(-d);
K<u,v>:=PolynomialRing(Q,2);
O:=MaximalOrder(Q);
IB:=IntegralBasis(Q);
w1:=IB[1];
w2:=IB[2];
Pol1:=(u*w1+v*w2)^n;
Pol1c:=(u*Conjugate(w1)+v*Conjugate(w2))^n;
Pnt1:=[x,1];Pnt2:=[1,x];
DW:=Denominator(w2);
if ((-d-1) mod 4) eq 0 then
q1:=q*DW;
else
q1:=q;
end if;
S2DC:=(2*q*a*C)*O;
IC:=C*O;
IFS2DC:={I: I in Factorization(S2DC)};
PrIS2DC:={Ip[1]:Ip in IFS2DC};
S2D:=(2*q*a)*O;
IFS2D:={I: I in Factorization(S2D)};
PrIS2D:={Ip[1]:Ip in IFS2D};
Gnew,G,phi:=smallSelmer(n,D,C,IC,PrIS2DC);
SetI:=
   SieveGCD(Gnew,phi,IFS2DC,O,n,S2DC,IFS2D);
GammaSet1:={};
for I in SetI do
st, elt:=IsPrincipal(I[1]);
```

```
st1, elt1:=IsPrincipal(I[2]);
if st then
GammaSet1:=GammaSet1 join {elt};
else
GammaSet1:=GammaSet1 join {elt1};
end if;
end for;
LUni:=UniSet(Q,n);
GammaSet2:={g*u:u in LUni, g in GammaSet1};
GammaSet:=
        Gammapfunction(n,D,d,q1,GammaSet2,a);
STEqts:=
GamThEqtns(a,DW,n,GammaSet,Pol1,Pol1c,Pnt1,Pnt2);
STEqts:={@tp:tp in STEqts| CoefTeste(tp,q1)
            and LocalThueEquation(tp, q1)@}
STEqts:={@tp:tp in STEqts|
    xFinThueEquations(tp, D1,D2,D3,n)@};
SetofSolutions:={};
for th in STEqts do
SolThue:=ThueEqtsMethods(th,q1,D,C,DW);
SetofSolutions:=SetofSolutions join SolThue;
end for;
printf "the solutions are [X,Y]:= %o\n",D1,D2,D3,n,
        SetofSolutions;
else
printf "we are working over the rationals field\n";
RaDn:=&*[p^n:p in PrimeBasis(2*q)];
S:=CartesianPower(Divisors(RaDn),2);
SI:=[v:v in S|PrimeBasis(v[1]) eq PrimeBasis(v[2])
        and (IsDivisibleBy(2*q,GCD(v[1],v[2])))
        and (IsPower(v[1]*v[2],n))];
Vaz:={};
```

```
for v in SI, c1 in Divisors(Abs(C)) do
c2:=C div c1;
r:=v[1]*c1;s:=v[2]*c2;
if IsDivisibleBy(2*q,GCD(r,s)) then
fq:=r*x^n-s;fx:=r*x^n+s;
t:={[fq,fx,1]};
t:={tp: tp in t |  LocalThueEquation(tp,2*q)
  and xFinThueEquations(tp, D1,D2,D3,n)};
Vaz:= Vaz join t;
end if;
end for;
STEqts:=Vaz;#STEqts;
SetofSolutions:={};
for th in STEqts do
SolThue:=ThueEqtsMethods(th,2*q,D,C,2);
SetofSolutions:=SetofSolutions join SolThue;
end for;
SetofSolutions:=SetofSolutions join {[q,0],[-q,0]};
printf "the solutions are [X,Y]:= %o\n",D1,D2,D3,n,
        SetofSolutions;
end if;
end if;
end for;
end for;
```

B.4 Code for the Modular Approach

In this section we presented the code to implement the modular approach as it was presented in Chapter 3.

B.4.1 The trace of the Frey curves

The following function has as output the Frobenius trace of the Frey curve $E(t)$ or $F(t)$ for a prime l and $0 \leq t \leq l-1$, such that $E(t)$ and $F(t)$ are well defined.

```
CongruenceEllipticCurves:=function(D,l,ta)
L:=[i:i in [1..l]|(i^2-D) mod l ne 0];
E:=[EllipticCurve([0,2*i,0,t*i^2+(-1)^ta*D,0]):i in L];
FroTr:=[Integers()!FrobeniusTraceDirect(E[i],l):i in [1..#L]];
return FroTr, L;
end function;
```

B.4.2 The signature of the equation $x^2 - D = y^n$

The following function given the input D gives all possible signatures of the equation $x^2 - D = y^n$, as we have seen in Lemma 3.3.1

```
Signature:=function(D)
S:=[[a,b]:a,b in Divisors(D)|a^2*b eq D and Gcd(a,b) eq 1];
S1:=[];
for P in S do
if IsEven(P[1]) then
if IsDivisibleBy(P[2]-1,8) then
S1:=S1 cat [P];
end if;
else
S1:=S1 cat [P];
end if;
end for;
S2:=[];
for P in S1 do
if P[1] ne 1 then
F:=Factorization(P[1]);
```

```
F:=[a[1]: a in F | IsOdd(a[1])];
if #F gt 0 then
R:=&+[KroneckerSymbol(P[2],q): q in F];
else
R:=0;
end if;
if R eq #F then
S2:=S2 cat [P];
end if;
else
S2:=S2 cat [P];
end if;
end for;
return S2;
end function;
```

B.4.3 Levels of the Frey curves

The following function given an integer n and a set of finite primes S, returns as output $\mathrm{Rad}_S(n)$. The function `Primefactors` was already defined in section B.3.1.

```
RadicalNumber:=function(D,S)
if D eq 0 then
return 0;
else
if Abs(D) eq  1 then
return 1
else
Rad:=&*[p:p in Primefactors(D) and p notin S];
return Rad;
end if;
```

```
end if;
end function;
```

This function given D and the signature (d_1, d_2), returns the levels predicted the by level lowering.

```
NewLevel:=function(D,d1,d2)
D1:=RadicalNumber(D,{2});
if IsDivisibleBy(D,4) then
v1:=Valuation(d1,2);
v2:=Valuation(d2,2);
if v2 gt 0 then
NLE:=[2^6*D1];
T:=[];
if v2 eq 2 then
if IsDivisibleBy(d2-4,16) then
T:=T cat [4];
else
t:=T cat [2];
end if;
end if;
if v2 eq 3 then
T:=T cat [5];
end if;
if (v2-4)*(v2-5) eq 0 then
T:=T cat [3];
end if;
if v2 eq 6 then
T:=T cat [0];
end if;
if v2 ge 7 then
t:=1;
end if;
```

```
NLF:=[(2^t)*D1:t in T];
end if;
if v2 eq 0 then
NLF:=[2^6*D1];
if v1 eq 1 then
T:=[1,3];
end if;
if v1 ge 2 then
T:=[1,3,5];
end if;
NLE:=[2^t*D1:t in T];
end if;
end if;
if IsDivisibleBy(D-1,4) then
if d2 mod 4 eq 1 then
te:=6;
tf:=5;
else
te:=5;tf:=6;
end if;
NLE:=[2*D1,2^te*D1;
NLF:=[2^6*D1,2^tf*D1];
end if;
if IsDivisibleBy(D-2,4) then
NLE:=[D1*2^7];NLF:=[2^7*D1];
end if;
if IsDivisibleBy(D-3,4) then
NLE:=[2^5*D1];NLF:=[2^6*D1];
end if;
return NLE,NLF;
end function;
```

B.4.4 Cuspforms and level lowering

This function just gathers all the newforms of possible different levels associated to a signature (d_1, d_2).

```
NewCuspforms:=function(NLE,NLF)
cuspE:=[**];cuspF:=[**];
for N in NLE do
cuspE:=cuspE cat Newforms(CuspForms(N));
end for;
for N in NLF do
cuspF:=cuspF cat Newforms(CuspForms(N));
end for;
return cuspE, cuspF;
end function;
```

The two following functions just implement the result of Proposition 3.3.2 to check for which possible primes p the equation $x^2 - D = y^p$ might have a solution.

```
CuspTeste:=function(f,N,SE,D,d2,PWofE,teste,res)
powersofE:={};l:=3;
while l le 150 do
if IsPrime(l) then
if IsDivisibleBy(2*D,l) eq false then
FroTr, L:=CongruenceEllipticCurves(d2,l,teste);
cl:=Coefficient(f,l);primos1:=[];
resto:=Lcm([Integers()!(Norm(cl-FroTr[i])): i in [1..#L]]);
if resto ne 0 then
if KroneckerSymbol(d2,l) eq 1 then
resto:=Lcm(resto,Integers()!Norm((l+1)^2-cl^2));
end if;
end if;
if res eq 1 then
```

```
resto:=resto*l;
end if;
if resto ne 0 then
primos:=Primefactors(resto);
else
primos:={p:p in [7..150]|IsPrime(p)};
end if;
printf "for prime %o we have that B_l(f) is %o, with prime
        factors %o \n",l,resto,primos;
possiblepowers:={l:l in primos|l ge 7};
if #powersofE eq 0 then
if #possiblepowers eq 0 then
if (l-7) ne 0 then
novait:=201;
else
powersofE:={7};novait:=2;
end if;
else
powersofE:=powersofE join possiblepowers;
novait:=2;
end if;
else
powersofE:= powersofE meet possiblepowers;
if #powersofE eq 0 then
novait:=150;
else
novait:=2;
end if;
end if;
else
novait:=2;
end if;
```

```
else
novait:=2;
end if;
expoente:=l;
l:=l+novait;
end while;
if IsPrime(expoente) then
p:=expoente;
else
Maximo:=Max(powersofE);
LPw:=Min(powersofE);
novait:=l;
end if;
printf "\n for the newform %o of level %o defined over the field %o
        we have the following possibilities of powers %o \n\n", f,
        N, BaseField(f), powersofE;
if #powersofE ge 1 then
SE:=SE cat [*f*];PWofE:=PWofE cat [powersofE];
end if;
return SE, PWofE;
end function;


LoweringTeste:=function(D,d2,cuspE,teste)
SE:=[* *];PWofE:=[];
for i in [1..#cuspE] do
f:=cuspE[i][1]; N:=Level(f); K:=BaseField(f);
if #Basis(K) eq 1 then
res:=0;
E:=EllipticCurve(f);
else
res:=1;
end if;
```

```
printf "we are testing the newform %o defined over %o\n",f,K;
SE, PWofE:=CuspTeste(f,N,SE,D,d2,PWofE,teste,res);
end for;
return SE,PWofE;
end function;
```

B.4.5 Kraus methods

The following functions are used to implement the Kraus methods (see section 3.3.3) to check if a newform f might arise or not from a solution of the equation $x^2 - D = y^p$. Some of the functions used by the following functions were already defined in section B.3.3.

```
NormTest:=function(alzet,cl,p,l)
if l mod 4 eq 1 then
return IsDivisibleBy(Integers()!(Norm(alzet-cl)),p);
else
return IsDivisibleBy(Integers()!(Norm(alzet^2-cl^2)),p);
end if;
end function;

NormTestR:=function(alzet,cl,p,l)
if l mod 4 eq 1 then
return (alzet-cl) eq 0;
else
return (alzet^2-cl^2) eq 0;
end if;
end function;

krauslp:=function(l,p,cl,d1,d2,D,ta,Rat,E);
n:= (l-1) div p;
Fl:=GF(l);
if Rat then
```

```
El:=ChangeRing(E,Fl);
if (IsDivisibleBy(Integers()!(4-cl^2),p) eq false)
   or (KroneckerSymbol(d2,l) eq -1) then
g:=PrimitiveElement(Fl)^p;
zeta:=1/g;
for i in [0..(n-1)] do
zeta:=zeta*g;
tf, delta:=IsSquare(Fl!(zeta+D));
if tf then
delta:=Fl!(delta/d1);
Ed:=EllipticCurve([Fl|0,2*delta,0,ta*delta^2+(-1)^ta*d2,0]);
O:=Ed!0;
cont:=1;
while cont le 5 do
P:=Random(Ed);
if Trace(El)*P eq O then
cont:=cont +1;
else
cont:=10;
end if;
end while;
if cont eq 6 then
alzet:=Trace(Ed);
if NormTestR(alzet,cl,p,l) then
return false;
end if;
end if;
end if;
end for;
return true;
else
return false;
```

```
end if;
else
if (IsDivisibleBy(Integers()!Norm(4-cl^2),p) eq false)
or (KroneckerSymbol(d2,l) eq -1) then
g:=PrimitiveElement(Fl)^p;
zeta:=1/g;
for i in [0..(n-1)] do
zeta:=zeta*g;
tf, delta:=IsSquare(Fl!(zeta+D));
if tf then
delta:=Fl!(delta/d1);
alzet:=Trace(
    EllipticCurve([Fl|0,2*delta,0,ta*delta^2+(-1)^ta*d2,0]));
if NormTest(alzet,cl,p,l) then
return false;
end if;
end if;
end for;
return true;
else
return false;
end if;
end if;
end function;


krausp:=function(p,f,d1,d2,D,ta,Rat,E);
l:=1;
if Rat then
B:=Floor((p^2-4)/(4*p));
repeat
repeat
l:=l+2*p;
```

```
if l gt (p*B+1) then
return false,0;
end if;
until IsPrime(l) and
   (IsDivisibleBy(D,l) eq false);
cl:=FrobeniusTraceDirect(E,l);
until krauslp(l,p,cl,d1,d2,D,t,Rat,E);
else
B:=1000;
repeat
repeat
l:=l+2*p;
if l gt (p*B+1) then
return false,0;
end if;
until IsPrime(l) and
   (IsDivisibleBy(D,l) eq false);
cl:=Coefficient(f,l);
until krauslp(l,p,cl,d1,d2,D,ta,Rat,E);
end if;
return true, ((l-1) div p);
end function;


twotorsion:=function(f)
K:=BaseField(f);
if #Basis(K) eq 1 then
E:=EllipticCurve(f);
if IsDivisibleBy(#TorsionSubgroup(E),2) then
print "f is rational and has a non-trivial two-torsion subgroup";
return true, E;
else
print "f is rational but does not have a non-trivial two-torsion
```

```
        subgroup";
return false, [];
end if;
else
print "f is not rational";
return false, [];
end if;
end function;


Gam:=function(D,p,d,q)
Q<a>:=QuadraticField(d);
O:=MaximalOrder(Q);
IB:=IntegralBasis(Q);
w1:=IB[1];
w2:=IB[2];
w:=FundamentalUnit(Q);
A:=(2*a*q)*O;
C:=1;
S2DC:=(2*q*a*C)*O;
IC:=C*O;
IFS2DC:={I: I in Factorization(S2DC)};
PrIS2DC:={Ip[1]:Ip in IFS2DC};
S2D:=(2*q*a)*O;
IFS2D:={I: I in Factorization(S2D)};
PrIS2D:={Ip[1]:Ip in IFS2D};
Gnew,G,phi:=smallSelmer(p,D,C,IC,PrIS2DC);
SetI:=SieveGCD(Gnew,phi,IFS2DC,O,p,S2DC,IFS2D);
GammaSet1:={};
for I in SetI do
st, elt:=IsPrincipal(I[1]);
st1, elt1:=IsPrincipal(I[2]);
if st then
```

```
GammaSet1:=GammaSet1 join {elt};
else
GammaSet1:=GammaSet1 join {elt1};
end if;
end for;
LUni:=UniSet(Q,p);
GammaSet2:=[g*u:u in LUni, g in GammaSet1];
return GammaSet2,a ;
end function;


GamsetltlTest:=function(l,p,d1,d2,ta,a,b,f,q,L1,L2)
n:=(l-1) div p;
Fl:=GF(l);
F1,th1:=ResidueClassField(L1);
F2,th2:=ResidueClassField(L2);
cl:=Coefficient(f,l);
i:=0;
repeat
test1:=(th1(d1*i-q*a))^n;
test2:=(th2(d1*iq*a))^n;
rest1:=(th1(b))^n;
rest2:=(th2(b))^n;
if KroneckerSymbol(d2,l) eq 1 then
if IsDivisibleBy(i^2-d2,l) then
if IsDivisibleBy(Norm((l+1)^2-cl^2),p) then
if ((test1 eq rest1) or (test1 eq 0))
and ((test2 eq rest2) or (test2 eq 0)) then
return true;
else
i:=i+1;
end if;
else
```

```
i:=i+1;
end if;
else
al:=Trace(
    EllipticCurve([Fl|0,2*i,0,ta*i^2+d2*(-1)^ta,0]));
if IsDivisibleBy(Norm(al-cl),p) then
if ((test1 eq rest1) or (test1 eq rest1)) and
((test2 eq rest2) or (test2 eq rest2)) then
return true;
else
i:=i+1;
end if;
else
i:=i+1;
end if;
end if;
else
al:=Trace(EllipticCurve([Fl|0,2*i,0,ta*i^2+d2*(-1)^ta,0]));
if IsDivisibleBy(Norm(al-cl),p) then
if ((test1 eq rest1) or (test1 eq rest1))
and ((test2 eq rest2 ) or (test2 eq rest2 ) ) then
return true;
else
i:=i+1;
end if;
else
i:=i+1;
end if;
end if;
until i eq l;
return false;
end function;
```

```
Gamp:=function(p,D,d1,d2,f,ta)
if IsSquare(D) eq false then
d,q:=SquarefreeFactorization(D);
Gamset,a:=Gam(D,p,d,q);
S:=[];
GR:=[];
B:=100;
l:=1;
repeat
repeat
repeat
repeat
repeat
repeat
l:=l+2*p;
if l gt (p*B+1) then
return S, Gamset;
end if;
until IsPrime(l);
until (IsDivisibleBy(D,l) eq false);
until (KroneckerSymbol(d,l) eq 1);
st,L1,L2:=(LocInt(Gamset,l,a));
until st;
GN:=#Gamset;
Gamset:=[b:b in
    Gamset|tlTest(l,p,d1,d2,ta,a,b,f,q,L1,L2)];
GN2:=#Gamset;
if GN2 lt GN then
S:=Append(S,l);
end if;
until #Gamset eq 0;
return S, Gamset;
```

```
end if;
end function;


krausRange:=function(PE,PmE,f,d1,d2,D,ta,pBnd,CDEC);
K:=BaseField(f);
S:=[];
if #PE le 10 then
L1:=Min(PE);L2:=Max(PE);
else
L1:=10^8;
if #PmE le 10 then
L2:=Max(PmE);
else
L2:=pBnd;
end if;
end if;
if IsPrime(L1) eq false then
p:=NextPrime(L1);
else
p:=L1;
end if;
Rat,E:=twotorsion(f);Rat; E;
if Rat then
CremonaReference(CDEC,E);
end if;
GammaS:=[];
repeat
k,n:=krausp(p,f,d1,d2,D,ta,Rat,E);
if k eq false then
if IsSquare(D) then
S:=Append(S,p);
GammaSet:=[];
```

```
lGamma:=[];
GammaSet:=[];
else
lGamma, GammaSet:=Gamp(p,D,d1,d2,f,ta);
if #GammaSet gt 0 then
S:=Append(S,p);
GammaS:=GammaS cat [[*GammaSet,p*]];
end if;
end if;
print p, k, n, lGamma, GammaSet,
"Norms are", [Norm(a): a in GammaSet];
else
lGamma:=[]; GammaSet:=[];
end if;
p:=NextPrime(p);
until p gt L2;
S:=Seqset(S);
if #PE le 10 then
S:=S meet PE;
end if;
return S,GammaS;
end function;
```

B.4.6 The algorithm

To end this section,we present the algorithm used to test the Modular approach to equations $x^2 - D = y^p$. We have the algorithm for the case $D = 98$.

```
CDEC:=CremonaDatabase();
for D in [98] do
pBnd:=10^8;
Sign:=Signature(D);
```

```
for P in Sign do
d1:=P[1];
d2:=P[2];
SkrE:=[**];
PKrE:=[];
SkrF:=[**];
PKrF:=[];
printf "\n  the Curve X^2-%o=Y^p, with
   signature d1=%o and d2=%o\n\n ",D,d1,d2;
NLE, NLF:=NewLevel(D,d1,d2);
NE:=Seqset(NLE);
NF:=Seqset(NLF);
printf "\n  the levels for the newforms associated
  with the Frey curve Et are %o \n\n", NLE;
printf "\n  the levels for the newforms associated
with the Frey curve Ft are %o \n\n", NLF;
cuspE, cuspF:=NewCuspforms(NLE,NLF);
printf "\n  CuspE has %o newforms\n\n", #cuspE;
printf "\n  CuspF has %o newforms\n\n", #cuspF;
if (#cuspE*#cuspF) eq 0 then
printf "\n  the Curve X^2-%o=Y^p, with signature
d1=%o and d2=%o has no primitive solutions,
by non existence of newforms\n\n ",D,d1,d2;
else
if #cuspE lt #cuspF then
C1:=cuspF;
C2:=cuspE;
t1:=1;
t2:=0;
print "C1 is CuspF and C2 CuspE";
else
C1:=cuspE;
```

```
C2:=cuspF;
t1:=0;
t2:=1;
print "C1 is CuspE and C2 CuspF";
end if;
printf "\n  We are testing the Level Lowering
        for C1\n\n";
SE, PwofE:=LoweringTeste(D,d2,C1,t1);
if #SE eq 0 then
printf "\n  the Curve X^2-%o=Y^p, with
   signature d1=%o and d2=%o has no
   primitive solutions, by level lowering
   of C1\n\n ",D,d1,d2;
else
printf "\n  We are testing the Level Lowering
for C2\n\n";
SF, PwofF:=LoweringTeste(D,d2,C2,t2);
if #SF eq 0 then
printf "\n  the Curve X^2-%o=Y^p, with
   signature d1=%o and d2=%o has no
   primitive solutions, by level lowering
   of C2\n\n ",D,d1,d2;
else
PmE:={};
for i in [1..#PwofE] do
PmE:=PmE join PwofE[i];
end for;
PmF:={};
for i in [1..#PwofF] do
PmF:=PmF join PwofF[i];
end for;
if #(PmE meet PmF) eq 0 then
```

```
printf "\n the Curve X^2-%o=Y^p, with
   signature d1=%o and d2=%o has no
   primitive solutions, by level lowering
   of C1 + C2\n\n ",D,d1,d2;
else
SE;SF;
printf "\n for C1 we have left %o newforms
   to test and for C2 we have left %o newforms
   \n\n",#SE,#SF;
printf "\n We are testing the Methods II+III
   for C1\n\n";
GamE:=[];
GamF:=[];
for i in [1..#SE] do
f:=SE[i];
PE:=PwofE[i];
N:=Level(f);
K:=BaseField(f);
B:=Basis(K);
 printf "\n testing the modular form f=%o of level=%o
 for the curve C1\n\n", f, N;
PE,GE:=
 krausRange(PE,PmF,f,d1,d2,D,t1,pBnd,CDEC);
if #PE gt 0 then
SkrE:=SkrE cat [*f*];
PKrE:=PKrE cat [PE];
GamE:=GamE cat [GE];
end if;
end for;
if #SkrE gt 0 then
printf "\n We are testing the Methods II+III
for C2\n\n";
```

```
for i in [1..#SF] do
f:=SF[i];
PE:=PwofF[i];
N:=Level(f);
K:=BaseField(f);
B:=Basis(K);
printf "\n testing the modular form f=%o of
level=%o for the curve C2\n\n", f, N;
PE,GE:=
 krausRange(PE,PmE,f,d1,d2,D,t2,pBnd,CDEC);
if #PE gt 0 then
SkrF:=SkrF cat [*f*];
PKrF:=PKrF cat [PE];
GamF:=GamF cat [GE];
end if;
end for;
if #SkrF eq 0 then
printf "\n the Curve X^2-%o=Y^p, with signature
   d1=%o and d2=%o has no primitive solutions
    by kraus methods\n\n",D,d1,d2;
else
IE:=[i: i in [1..#SkrE]|
   #Basis(BaseField(SkrE[i])) ge 1];
IF:=[i: i in [1..#SkrF]|
   #Basis(BaseField(SkrF[i])) ge 1];
Cusps:=[[*SkrE[i],g*]:i in IE, g in SkrF]
   cat [[*f,SkrF[i]*]:f in SkrE, i in IF];
Powers:=[PKrE[i] meet PKrF[j]: i in IE, j in IF]
   cat [E meet PKrF[i]: E in PKrE, i in IF];
printf "\n The possible cusps and powers for
which the curve X^2-%o=Y^p with signature
d1=%o, d2=%o might have solution are %o %o,
```

```
\nwith Gammas:%o\n %o\n\n", D,d1,d2,
Cusps, Powers,GamE,GamF;
end if;
else
printf "\n the Curve X^2-%o=Y^p, with signature
   d1=%o and d2=%o has no primitive solutions
   by kraus methods\n\n",D,d1,d2;
end if;
end if;
end if;
end if;
end if;
end for;
end for;
```

B.5 Code for Linear forms in logarithms

In this section we presented the functions that were used to obtain the bounds given by linear forms in logarithms in Chapter 4.

B.5.1 Calculating $\gcd$, α's and logarithmic heights

. In this section we present functions that are need to calculate the constant c, α as the logarithmic height of α, given by the Lemma 4.3.1.

The first function obtains the constant $c = \gcd(x + q\sqrt{d}, x - \sqrt{d})$, given by the Lemma mentioned above.

```
dValue:=function(D,P)
d1:=P[1];d2:=P[2];
if (D mod 4) eq 2 then
return [d1];
```

```
end if;
if (D mod 4) eq 3 then
return [d1];
end if;
if (D mod 4) eq 0 then
if IsEven(d2) then
return [d1];
else
return [2*d1];
end if;
end if;
if (D mod 4) eq 1 then
return [d1, 2*d1];
end if;
end function;
```

The following function help us to choose the fundamental unit u of $\mathbb{K}_D$, such that $\log \overline{u} = \max\{\log|u|, \log|\overline{u}|\}$.

```
MaxUnit:=function(u)
RR:=RealField();
v1:=RR!Conjugate(u);
u1:=RR!u;
u2:=RR!(-1*u);
v2:=RR!Conjugate(-1*u);
Rl:=[[u1,AbsoluteLogarithmicHeight(u)],
  [u2,AbsoluteLogarithmicHeight(-1*u)],
  [v1,AbsoluteLogarithmicHeight(Conjugate(u))],
  [v2,AbsoluteLogarithmicHeight(Conjugate(-1*u))]];
Ul:=[u,-1*u,Conjugate(u),Conjugate(u)];
N:=[Rl[i]:i in [1..4]|Rl[i][1] gt 1];
N2:=[Ul[i]:i in [1..4]|Rl[i][1] gt 1];
M:=Max([Log(N[i][1]): i in [1..#N]]);
```

```
for i in [1..#N] do
if Log(N[i][1]) eq M then
return N[i][1], N[i][2], N2[i];
end if;
end for;
end function;
```

The following functions helps us to calcultae α verifying the hypothesis of the Lemma 4.3.1, including the fact that $\alpha < 1$.

```
AlphaZero:=function(I)
L:=[P:P in Divisors(I)|(P*Conjugate(P) eq I)
  and (P ne Conjugate(P))];
T:={};
for P in L do
if #T eq 0 then
T:=T join {P};
else
if ((P in T) eq false) and
   ((Conjugate(P) in T) eq false) then
T:=T join {P};
end if;
end if;
end for;
return T;
end function;


IdealOrder:=function(I,cl)
DivCl:=Divisors(cl);
for d in DivCl do
st,elt:=IsPrincipal(I^d);
st2,elt2:=IsPrincipal(Conjugate(I)^d);
if (st and st2) then
```

```
if Abs(RealField()!Conjugate(elt)/RealField()!elt)
  lt Abs(RealField()!Conjugate(elt2)/RealField()!elt2)
  then
return elt, d;
else
return elt2, d;
end if;
end if;
end for;
end function;


A1Value:=function(I,cl,v,uc)
T:=AlphaZero(I);RR:=RealField();
A1:=[];
for I in T do
elt,k1:=IdealOrder(I,cl);
alpha:=Conjugate(elt)/elt;
alpha1:=(RR!Conjugate(elt))/(RR!elt);
k:= 2 div k1;
s:=Floor(1-Log(Abs(alpha1))/(2*Log(v)));
r:=Floor(-1*Log(Abs(alpha1))/(2*Log(v))-1/-s)+1;
elt1:=elt*Conjugate(uc)^(r+s);
alpha:=Conjugate(elt1)/elt1;
alpha1:=(RR!Conjugate(elt1))/(RR!elt1);
if Abs(alpha1) lt 1 then
alpha:=alpha^(-1);alpha1:=1/alpha1;
end if;
if alpha1 lt 0 then
alpha1:=-1*alpha1;
alpha:=-1*alpha;
end if;
if alpha1 gt 0 then
```

```
if k eq 1 then
ha:=AbsoluteLogarithmicHeight(alpha);
A1:=A1 cat [Max(2*ha,0.16)];
else
hb:=AbsoluteLogarithmicHeight(alpha);
ha:=AbsoluteLogarithmicHeight(alpha^2);
k:=1;
alpha1:=alpha1^2;
A1:=A1 cat [Max(2*hb,0.16)];
end if;
else
if k eq 1 then
ha:=AbsoluteLogarithmicHeight(-1*alpha);
A1:=A1 cat [Max(2*ha,0.16)];
alpha1:=-1*alpha1;
else
hb:=AbsoluteLogarithmicHeight(-1*alpha);
ha:=AbsoluteLogarithmicHeight(alpha^2);
k:=1;
alpha1:=alpha1^2;
A1:=A1 cat [Max(2*hb,0.16)];
end if;
end if;
end for;
if #A1 gt 0 then
return A1,k, alpha1,ha;
else
return A1,0,0,0;
end if;
end function;
```

B.6 Zeros of a real function

The following function is a version of the bisection method of a root-finding algortihm, which will be used to obtain the lower bounds.

```
FZeros:=function(F,a,b,Error)
if (F(a)*F(b)) lt 0 then
while Abs(a-b) ge Error do
c:=RealField()!((a+b)/2);
if F(c) eq 0 then
return true, c;
else
if (F(a)*F(c)) gt 0 then
a:=c;
else
b:=c;
end if;
end if;
end while;
if F(a) gt 0 then
return true, b;
else
return true, b;
end if;
else
if F(a) lt 0 then
return true, b;
else
return true, b;
end if;
end if;
end function;
```

B.6.1 Linear form in two logarithms

The following functions implement results of the Proposition 4.3.2. We have four different versions, one for the two linear forms:

$$\Lambda_2 := 2r\log(\overline{u}) + p\log(\lambda),$$
$$\Lambda_3' := \log\left(\overline{u}^{t_1 2r}\overline{\alpha}^{-kq't_2}\right) - p\log\left(\overline{\lambda}^{t_1}\overline{\alpha}^{-\delta k}\right) \text{ and}$$
$$t_1\Lambda_3 := \log(\overline{u}^{t_1 2r}\overline{\alpha}^{-kq't_2}) - p\log(\overline{\lambda}^{t_1}\overline{\alpha}^{-\delta k}).$$
$$t_2\Lambda_3 = log\left(\overline{\alpha}^{-kt_2}\overline{u}^{t_1 s_1'}\right) - p\log\left(\overline{u}^{-s_1}\overline{\lambda}^{t_2}\right).$$

We make the distinction in order to have better implementations of the method for each case.

```
LinearFormsinTwoLogs:=function(B,v,hv,D1,D2,i)
D:=D1^2*D2;
B1:=B;km:=100;
kc:=40;
RI:=[5000..100000];
kf:=0;
Kf:=0;
Lf:=0;
rf:=0;
hf:=0;
kmf:=0;
for r1 in RI do
r:=r1/1000;
l:=Log(r);
a2:=Max([4,2.7*l,(r-1)*Log(v)+4*hv]);
yB:=10^3;
delta:=(10^3-Sqrt(D))/(10^3+Sqrt(D));
```

```
a1:=Max([4,2.7*l,
2*Log((Sqrt(yB)-1)^2)+(r+1)*(2*(B-1)*Log(v)-Log(delta))/B]);
if (a1*a2 ge 20*l^2) and (a1 gt 0) and (a2 gt 0) then
k:=kc/(90*l^2);
K:=0;
j:=1;
st:=false;
while st eq false do
if j gt 1 then
k1:=Floor(K/10);
resto:=K/10-k1;
if resto gt 0.5 then
km:=k1*10+5;
else
km:=k1*10;
end if;
end if;
f:=Log((1+Sqrt(km-1))*Sqrt(km)/(km-1))+
Log(km)/(6*km*(km-1))+3/2+
Log(3/4)+Log(km/(km-1))/(km-1);
h:=Max([1,1.5*l,
  2*(Log(B/a2+(2*B-2)/a1)+Log(l)+f)+0.0262]);
L:=2+Floor(2*h/l);
K:=1+Floor(k*L*a1*a2);
if K ge km then
if (K-km) lt 5 then
st:=true;
else
if j ge 3 then
st:=true;
else
st:=false;
```

```
end if;
end if;
else
st:=false;
end if;
j:=j+1;
end while;
if L ge 5 then
pBnd:=PreviousPrime(
Floor(
2*(l*k*L^2*a1*a2+
Max([l*(L-0.5)+Log(L^2*(1+Sqrt(k)*a2)),2*Log(2)])
+Log(2.2*Sqrt(D)))/Log((Sqrt(yB)-1)^2)
)
);
if pBnd lt B1 then
B1:=pBnd;
Kf:=K;
rf:=r1;
kf:=kc;
hf:=h;
Lf:=L;
kmf:=km;
end if;
end if;
end if;
end for;
return B1,Kf,Lf,hf,rf,kf,kmf;
end function;


Lf2L1:=function(B,v,hv,alpha,ha,D1,D2,BTS,i)
D:=D1^2*D2;
```

```
B1:=B;km:=100;
kc:=40;
RI:=[5000..200000];
kf:=0;
Kf:=0;
Lf:=0;
rf:=0;
hf:=0;
kmf:=0;
for r1 in RI do
r:=r1/1000;l:=Log(r);
a2:=Max([4,2.7*l,
  r*Abs(Log(v^BTS*alpha^(-1)))
   -Log(v^BTS*alpha^(-1))+4*(hv*BTS+ha)]);
yB:=(Sqrt(B)-1)^2;
delta:=(10^9-Sqrt(D))/(10^9+Sqrt(D));
a1:=Max([4,2.7*l,
  2*Log((Sqrt(yB)-1)^2)+
  (r+1)*(2*(B1-1)*Log(v)-Log(delta))/B1]);
if (a1*a2 ge 20*l^2) and
(a1 gt 0) and (a2 gt 0) then
k:=kc/(90*l^2);
K:=0;
j:=1;
st:=false;
while st eq false do
if j gt 1 then
k1:=Floor(K/10);
resto:=K/10-k1;
if resto gt 0.5 then
km:=k1*10+5;
else
```

```
km:=k1*10;
end if;
end if;
f:=Log((1+Sqrt(km-1))*Sqrt(km)/(km-1))
+Log(km)/(6*km*(km-1))+3/2+Log(3/4)
+Log(km/(km-1))/(km-1);
h:=Max([1,1.5*l,
2*(Log(B1/a2+(2*B1-2)/a1)+Log(l)+f)+0.0262]);
L:=2+Floor(2*h/l);
K:=1+Floor(k*L*a1*a2);
if K ge km then
if (K-km) lt 5 then
st:=true;
else
if j ge 3 then
st:=true;
else
st:=false;
end if;
end if;
else
st:=false;
end if;
j:=j+1;
end while;
if L ge 5 then
F1:=map<RealField() -> RealField() |
  x :-> x -2*(l*k*L^2*a1*a2+
  Max([l*(L-0.5)+Log(L^2*(1+Sqrt(k)*a2)),2*Log(2)])
  +Log(2.2*Sqrt(D)))/Log((Sqrt(x)-1)^2)>;
st3,pBnd:=Fzeros(F1,10^3,B1,1);
if st3 then
```

```
if PreviousPrime(pBnd) lt B1 then
B1:=PreviousPrime(pBnd);
Kf:=K;
rf:=r1;
kf:=kc;
hf:=h;
Lf:=L;
kmf:=km;
end if;
end if;
end if;
end if;
end for;
return B1,Kf,Lf,hf,rf,kf,kmf;
end function;


Lf2L2pt2:=
  function(B,v,hv,alpha,ha,D1,D2,BR,BS,BT,i)
D:=D1^2*D2;
B1:=B;
km:=100;
kc:=40;
RI:=[5000..200000];
kf:=0;
Kf:=0;
Lf:=0;
rf:=0;
hf:=0;
kmf:=0;
for r1 in RI do
r:=r1/1000;l:=Log(r);
a2:=Max([4,2.7*l,
```

```
   r*Abs(BR*Log(v)-BS*Log(alpha))-BR*Log(v)
   +BS*Log(alpha)+4*(hv*BR+ha*BS)]);
yB:=(Sqrt(B)-1)^2;
delta:=(10^9-Sqrt(D))/(10^9+Sqrt(D));
log1:=(Log(1/alpha)+2*(B1-1)*Log(v)-Log(delta))/B1;
log2:=(-1*Log(1/alpha)-2*(B1-1)*Log(v))/B1;
hl:=Log((Sqrt(yB)-1)^2)/2 +log1/(2*B1);
a1:=Max([4,2.7*l,r*Abs(-BT*Log(alpha)+BS*log1)+
   BT*Log(alpha)-BS*log2+4*(ha*BT+hl*BS)]);
if (a1*a2 ge 20*l^2) and (a1 gt 0)
   and (a2 gt 0) then
k:=kc/(90*Log(r)^2);
K:=0;
j:=1;
st:=false;
while st eq false do
if j gt 1 then
k1:=Floor(K/10);
resto:=K/10-k1;
if resto gt 0.5 then
km:=k1*10+5;
else
km:=k1*10;
end if;
end if;
f:=Log((1+Sqrt(km-1))*Sqrt(km)/(km-1))+
   Log(km)/(6*km*(km-1))+3/2+Log(3/4)+
   Log(km/(km-1))/(km-1);
h:=Max([1,1.5*l,2*(Log(B1/a2+(2*B1-2)/a1)
   +Log(l)+f)+0.0262]);
L:=2+Floor(2*h/l);
K:=1+Floor(k*L*a1*a2);
```

```
if K ge km then
if (K-km) lt 5 then
st:=true;
else
if j ge 3 then
st:=true;
else
st:=false;
end if;
end if;
else
st:=false;
end if;
j:=j+1;
end while;
if L ge 5 then
F1:=map<RealField() -> RealField() |
   x :-> x -2*(l*k*L^2*a1*a2+
   Max([l*(L-0.5)+Log(L^2*(1+Sqrt(k)*a2)),2*Log(2)])
   +Log(2.2*Sqrt(D))+Log(BS))/Log((Sqrt(x)-1)^2)>;
st3,pBnd:=Fzeros(F1,10^3,B1,1);
if st3 then
if PreviousPrime(pBnd) lt B1 then
B1:=PreviousPrime(pBnd);
Kf:=K;
rf:=r1;
kf:=kc;
hf:=h;
Lf:=L;
kmf:=km;
end if;
end if;
```

```
end if;
end if;
end for;
return B1,Kf,Lf,hf,rf,kf,kmf;
end function;


Lf2L2pt1:=function(B,v,hv,alpha,ha,D1,D2,BR,BS,BT,i)
D:=D1^2*D2;
B1:=B;
km:=100;
kc:=40;
RI:=[5000..200000];
kf:=0;
Kf:=0;
Lf:=0;
rf:=0;
hf:=0;
kmf:=0;
for r1 in RI do
r:=r1/1000;
l:=Log(r);
a2:=Max([4,2.7*l,
    r*Abs(BR*Log(v)-BS*Log(alpha))-BR*Log(v)+
    BS*Log(alpha)+4*(hv*BR+ha*BS)]);
yB:=(Sqrt(B)-1)^2;
delta:=(10^9-Sqrt(D))/(10^9+Sqrt(D));
log1:=(Log(1/alpha)+2*(B1-1)*Log(v)-Log(delta))/B1;
log2:=(-1*Log(1/alpha)-2*(B1-1)*Log(v))/B1;
hl:=Log((Sqrt(yB)-1)^2)/2 +log1/(2*B1);
a1:=Max([4,2.7*l,
    r*Abs(-BT*Log(v)+BS*log1)+BT*Log(v)
    -BS*log2+4*(hv*BT+hl*BS)]);
```

```
if (a1*a2 ge 20*l^2) and (a1 gt 0)
  and (a2 gt 0) then
k:=kc/(90*Log(r)^2);
K:=0;
j:=1;
st:=false;
while st eq false do
if j gt 1 then
k1:=Floor(K/10);
resto:=K/10-k1;
if resto gt 0.5 then
km:=k1*10+5;
else
km:=k1*10;
end if;
end if;
f:=Log((1+Sqrt(km-1))*Sqrt(km)/(km-1))
  +Log(km)/(6*km*(km-1))+3/2+Log(3/4)
  +Log(km/(km-1))/(km-1);
h:=Max([1,1.5*l,
   2*(Log(B1/a2+(2*B1-2)/a1)+Log(l)+f)+0.0262]);
L:=2+Floor(2*h/l);
K:=1+Floor(k*L*a1*a2);
if K ge km then
if (K-km) lt 5 then
st:=true;
else
if j ge 3 then
st:=true;
else
st:=false;
end if;
```

```
end if;
else
st:=false;
end if;
j:=j+1;
end while;
if L ge 5 then
F1:=map<RealField() -> RealField() |
   x :-> x -2*(l*k*L^2*a1*a2+
   Max([l*(L-0.5)+Log(L^2*(1+Sqrt(k)*a2)),2*Log(2)])
   +Log(2.2*Sqrt(D))+Log(BR))/Log((Sqrt(x)-1)^2)>;
st3,pBnd:=Fzeros(F1,10^3,B1,1);
if st3 then
if PreviousPrime(pBnd) lt B1 then
B1:=PreviousPrime(pBnd);
Kf:=K;
rf:=r1;
kf:=kc;
hf:=h;
Lf:=L;
kmf:=km;
end if;
end if;
end if;
end if;
end for;
return B1,Kf,Lf,hf,rf,kf,kmf;
end function;
```

B.6.2 Linear form in three logarithms

The following functions are used to implement the result of the Theorem 4.2 to obtain bounds for linear forms in three logarithms.

The first two functions are to calculate the two linear forms that we have when we are in **Case 1** or **Case 2** of the afore mentioned Theorem. The third one is the implementation of the method to obtain lower bounds for the linear forms in logarithms, using Theorem 4.2.

```
Condition3pt1:=
  function(Bl1,v,hv,alpha,ha,D1,D2,BTS)
B2:=7;
while B2 lt Bl1 do
if B2 gt 7 then
Bl1:=B2;
end if;
B2,K1,L1,h,r1,k,km:=
  Lf2L1(Bl1,v,hv,alpha,ha,D1,D2,BTS,i);
end while;
return B2;
end function;

Condition3pt2:=
  function(Bl1,v,hv,alpha,ha,D1,D2,BR,BS,BT,a1,a2)
B2:=7;
while B2 lt Bl1 do
if B2 gt 7 then
Bl1:=B2;
end if;
if a1 lt a2 then
B2,K2,L2,h,r2,k,km:=
  Lf2L2pt1(Bl1,v,hv,alpha,hv,D1,D2,BR,BS,BT,j);
```

```
else
B2,K2,L2,h,r2,k,km:=
  Lf2L2pt2(Bl1,v,hv,alpha,hv,D1,D2,BR,BS,BT,j);
end if;
end while;
return B2;
end function;


LinearFormin3Logs:=
  function(alpha,ha,v,hv,D1,D2,B,delta)
D:=D1^2*D2;
Bmig:=B;
r1:=0; r2:=0; r3:=0;
s1:=0; s2:=0; s3:=0;
t1:=0; t2:=0; t3:=0;
Chir:=0; mv:=0; kv:=0;
rh:=0; Lv:=0;
BTh:=0; BRh:=0; BSh:=0;
BTRh:=0; BTSh:=0;
a1h:=0; a2h:=0;
Bmin:=0;
Rho:=30;
while Rho le 200 do
Rh:=Rho/10;
Rh;
L:=5;
PL:=0;
while L le 1500 do
Chi:=5;
Mt:=1;
chi:=Chi/10;
Bt:=0;
```

```
r1t:=0; r2t:=0; r3t:=0;
s1t:=0; s2t:=0; s3t:=0;
t1t:=0; t2t:=0; t3t:=0;
Chit:=0; mt:=0; kt:=0;
rht:=0; Lt:=0;
BTt:=0; BRt:=0; BSt:=0;
BTRt:=0; BTSt:=0;
a1t:=0; a2t:=0;
B1:=7;
B:=Bmig;
a1:=(Rh-1)*Log(alpha)+4*ha;
a2:=(Rh-1)*Log(v)+4*hv;
a3:=(Rh+1)*Max(Log(1/alpha)+2*(B-1)*Log(v)-Log(delta),
    -1*Log(1/alpha)-2*(B-1)*Log(v))/B
  +2*Log((Sqrt(B)-1)^2);
if (a1 ge 1) and (a2 ge 1) and (a3 ge 1) then
mMax:=Max([3/(L*a1*a2*a3),8/(a^3*L*chi^4),
    L^2/(4*a^3)]);
mfun:=map<RealField()->RealField()|
x:-> (Floor(x*L*a1*a2*a3)*L/2+L/4-1
-2*Floor(x*L*a1*a2*a3)/(3*L))*Log(Rh)
- (3*Log(Floor(x*L*a1*a2*a3)^2*L)+(1/4
-Floor(x*L*a1*a2*a3)^2*L/
(12*(Floor(a2*a3*(chi*x*L)^(2/3))
+Floor(a2*a3*2^(1/3)*(x*L)^(2/3))
+Floor(a2*a3*(6*x^2)^(1/3)*L)+1)*
(Floor(a1*a3*(chi*x*L)^(2/3))
+Floor(a1*a3*2^(1/3)*(x*L)^(2/3))
+Floor(a1*a3*(6*x^2)^(1/3)*L)+1)*
(Floor(a2*a1*(chi*x*L)^(2/3))+
Floor(a2*a1*2^(1/3)*(x*L)^(2/3))+
Floor(a2*a1*(6*x^2)^(1/3)*L)+1)))*L*
```

```
(a1*(Floor(a2*a3*(chi*x*L)^(2/3))+
Floor(a2*a3*2^(1/3)*(x*L)^(2/3))+
Floor(a2*a3*(6*x^2)^(1/3)*L)+1)+
a2*(Floor(a1*a3*(chi*x*L)^(2/3))+
Floor(a1*a3*2^(1/3)*(x*L)^(2/3))+
Floor(a1*a3*(6*x^2)^(1/3)*L)+1)+
a3*(Floor(a2*a1*(chi*x*L)^(2/3))+
Floor(a2*a1*2^(1/3)*(x*L)^(2/3))+
Floor(a2*a1*(6*x^2)^(1/3)*L)+1))+
2*(Floor(x*L*a1*a2*a3)-1)*(
Log((Floor(a2*a3*(chi*x*L)^(2/3))
+Floor(a2*a3*2^(1/3)*(x*L)^(2/3))
+Floor(a2*a3*(6*x^2)^(1/3)*L))/2
+(Floor(a1*a3*(chi*x*L)^(2/3))
+Floor(a1*a3*2^(1/3)*(x*L)^(2/3))
+Floor(a1*a3*(6*x^2)^(1/3)*L))/
(2*(2*B-2)))+2*Log(2*B-2)+
Log((Floor(a2*a1*(chi*x*L)^(2/3))+
Floor(a2*a1*2^(1/3)*(x*L)^(2/3))+
Floor(a2*a1*(6*x^2)^(1/3)*L))/2+
(Floor(a2*a3*(chi*x*L)^(2/3))+
Floor(a2*a3*2^(1/3)*(x*L)^(2/3))+
Floor(a2*a3*(6*x^2)^(1/3)*L))*
B/(2*(2*B-2)))
-4/(Floor(x*L*a1*a2*a3)^2-
Floor(x*L*a1*a2*a3))*(
Log(Floor(x*L*a1*a2*a3)-1)*
(Floor(x*L*a1*a2*a3)-1)/2+
(-3*Floor(x*L*a1*a2*a3)^2+
6*Floor(x*L*a1*a2*a3)-2)/4
)
)
```

```
-2*Log(Exp(1)/2))>;
st4,mT:=FZeros(mfun,mMax,10^5,10^(-15));
if mT eq 10^5 then
m1:=mMax;
else
m1:=mT;
end if;
for m in [ m1, (m1+Floor(m1)+1)/2,
  Floor(m1)+1,m1+1,(m1+Floor(m1)+1)/2+1,
  Floor(m1)+2] do
c1:=Max((chi*m*L)^(2/3),Sqrt(2*m*L/a));
c2:=Max(2^(1/3)*(m*L)^(2/3),Sqrt(m/a)*L);
c3:=(6*m^2)^(1/3)*L;
T1:=Floor(c1*a1*a2);
T2:=Floor(c2*a1*a2);
T3:=Floor(c3*a1*a2);
Tm:=Max(T1,T2);
T:=T1+T2+T3+1;
K:= Floor(m*L*a1*a2*a3);
R1:=Floor(c1*a2*a3);
R2:= Floor(c2*a2*a3);
R3:= Floor(c3*a2*a3);
S1:=Floor(c1*a1*a3);
S2:= Floor(c2*a1*a3);
Sm:=Max(S1,S2);
S3:= Floor(c3*a1*a3);
R:= R1+R2+R3+1;
S:= S1+S2+S3+1;
N:=L*K^2;
g:= 1/4-N/(12*R*S*T);
nu0:= Log((R-1)/2+(S-1)/(2*(2*B-2)));
eta0:= Log((T-1)/2+(S-1)*B/(2*(2*B-2)));
```

```
exp:=-4/(K*(K-1));
e:=Exp(1);
pi:=Pi(RealField());
v1:=(K*L/2+L/4-1-2/3*K/L)*Log(Rh)
  -3*Log(N)-g*L*(a1*R+a2*S+a3*T)
  -2*Log(e/2)-2*(K-1)*(2*Log(2*B-2)+
  eta0+nu0+2*Log(K)-3
  +2*Log(2*pi*K/Exp(3/2))/(K-1)
  -(2+6*pi^(-2)+Log(K))/(3*(K^2-K)));
if v1 gt 0 then
V:=Sqrt((R1+1)*(S1+1)*(T1+1));
M:=Max([R1+S1+1,R1+T1+1,S1+T1+1,chi*V]);
BTR:=Floor((R1+1)*(T1+1)/(M-T1));
BTS:=Floor((S1+1)*(T1+1)/(M-T1));
BR:=Floor((S1+1)*(T1+1)/(M-Max(T1,S1)));
BS:=Floor((R1+1)*(T1+1)/(M-Max(R1,T1)));
BT:=Floor((S1+1)*(R1+1)/(M-Max(S1,R1)));
F1:=map<RealField() -> RealField() |
x :-> x -2*(K*L*Log(Rh)+Log(L*Max([R,S,T]))
+Log(2.2*D1*Sqrt(D2)))/Log((Sqrt(x)-1)^2)>;
st3,Btry:=Fzeros(F1,10^3,B,1);
B1:=PreviousPrime(Floor(Btry));
if st3 and (B1 lt B) and (Tm lt B1) and
   (m*a1*a2*a3 ge 2) and (Sm lt B1) then
if Bt eq 0 then
r1t:=R1; r2t:=R2; r3t:=R3;
s1t:=S1; s2t:=S2; s3t:=S3;
t1t:=T1; t2t:=T2; t3t:=T3;
Chit:=chi; mt:=m; kt:=K;
rht:=Rh; Lt:=L;
BTt:=BT; BRt:=BR; BSt:=BS;
BTRt:=BTR; BTSt:=BTS;
```

```
a1t:=a1; a2t:=a2;
Bt:=B1;
else
if (Abs(BTS) lt Abs(BTSt)) and
(Abs(BR) lt Abs(BRt)) and (Abs(BS) lt Abs(BSt))
and (Abs(BT) lt Abs(BTt)) then
r1t:=R1; r2t:=R2; r3t:=R3;
s1t:=S1; s2t:=S2; s3t:=S3;
t1t:=T1; t2t:=T2; t3t:=T3;
Chit:=chi; mt:=m; kt:=K;
rht:=Rh; Lt:=L;
BTt:=BT; BRt:=BR; BSt:=BS;
BTRt:=BTR; BTSt:=BTS;
a1t:=a1; a2t:=a2;
Bt:=B1;
end if;
end if;
end if;
else
B1:=Bmig;
end if;
if (Bt lt Bmig) and (Bt gt 0) then
if Bmin eq 0 then
printf "p Bound:=%o, for rho:=%o, L:=%o, m:=%o,
  chi:=%o\n", rht, Bt,Lt,mt,Chit;mMax;
r1t:=R1; r2t:=R2; r3t:=R3;
s1t:=S1; s2t:=S2; s3t:=S3;
t1t:=T1; t2t:=T2; t3t:=T3;
Chit:=chi; mt:=m; kt:=K;
rht:=Rh; Lt:=L;
BTt:=BT; BRt:=BR; BSt:=BS;
BTRt:=BTR; BTSt:=BTS;
```

```
a1t:=a1; a2t:=a2;
Bt:=Bt;
else
if (Bt lt Bmin) then
printf "p Bound:=%o, for rho:=%o, L:=%o, m:=%o,
chi:=%o\n", rht, Bt, Lt, mt, Chit; mMax;
r1t:=R1; r2t:=R2; r3t:=R3;
s1t:=S1; s2t:=S2; s3t:=S3;
t1t:=T1; t2t:=T2; t3t:=T3;
Chit:=chi; mt:=m; kt:=K;
rht:=Rh; Lt:=L;
BTt:=BT; BRt:=BR; BSt:=BS;
BTRt:=BTR; BTSt:=BTS;
a1t:=a1; a2t:=a2;
Bt:=Bt;
end if;
end if;
end if;
end for;
end if;
L:=L+1;
end while;
Rho:=Rho+1;
end while;
B:=Bmig;
BC31:=Condition3pt1(Bmig, v, hv, alpha, ha, D1, D2, BTSh);
if BC31 lt B then
BC32:=Condition3pt2(
    Bmig, v, hv, alpha, ha, D1, D2, BRh, BSh, BTh, a1h, a2h);
if BC32 lt B then
Bmin3:=Max([BC32, BC31, Bmin]);
if Bmin3 lt B then
```

```
Bmig:=Bmin3;
return r1,r2,r3,s1,s2,s3,t1,t2,t3,Chir,mv,kv,rh,Lv,
 Bmig,BRh,BSh,BTh;
else
return 0,0,0,0,0,0,0,0,0,0,0,0,0,0,Bmig,0,0,0;
end if;
else
return 0,0,0,0,0,0,0,0,0,0,0,0,0,0,Bmig,0,0,0;
end if;
end if;
end function;
```

B.6.3 The Algorithm

We present now the algorithm to compute the bounds presented in the main body of this thesis, as well we have the implementation of the Matveev's results, as we presented in Thereom 4.1 and the following discussion.

```
for D in [17] do
D2,D1:=SquareFreeFactorization(D);
Q<a>:=QuadraticField(D2);
O:=MaximalOrder(Q);
u:=FundamentalUnit(Q);
v,hv,uc:=MaxUnit(u);
cl:=ClassNumber(Q);
SignD:=Signature(D);
for P in SignD do
dVal:=dValue(D,P);
printf "for D=%o we have the following possibilites
 for d: %o\n",D, dVal;
for d in dVal do
if d eq 1 then
```

```
A1:=[1];n:=2;alpha:=1;
else
n:=3;
A1,k,alpha,ha:=A1Value(d*O,cl,v,uc);
end if;
delta:=(10^9-Sqrt(D))/(10^9+Sqrt(D));
A2:=Max(2*hv,0.16);
e:=Exp(1);
Cn:=(16/Factorial(n))*(e^n)*(2*n+3)*(n+2)*
       (e*n/2)*(4*(n+1))^(n+1);
C0:=Log(e^(4.4*n+7)*n^(5.5)*4*Log(2*e));
C1:=3*e*Log(2*e);
if #A1 ge 1 then
for A in A1 do
omega1:=A*A2;
delta:=(10^9-Sqrt(D))/(10^9+Sqrt(D));
C5:=Cn*C0*omega1*2;
C6:=2*Log(2.2*D1*Sqrt(D2));
F1:=map<RealField() -> RealField() |
   x :-> x -2*(Log(C1*x)*C5*(Log((Sqrt(x)-1)^2)+
   Max(Log(1/alpha)+2*(x-1)*Log(v)-Log(delta),
   -Log(1/alpha)-2*(x-1)*Log(v))/x)-C6)/
   Log((Sqrt(x)-1)^2)>;
st3,B2:=Fzeros(F1,C5,10^15,1);
if (st3) then
B2:=Floor(B2+1);
B:=PreviousPrime(B2);
printf "for D=%o, with signature (d1,d2)=%o,
with d=%o, we have the following upper bound
for the primes p, by Matveev results, %o\n\n ",
D, P, d, B;
i:=1;
```

```
if n eq 2 then
B2:=7;
while B2 lt B do
if B2 gt 7 then
B:=B2;
end if;
B2,K,L,h,r,k,km:=
 LinearFormsinTwoLogs(B,v,hv,D1,D2,i);
printf "for D=%o, with signature (d1,d2)=%o,
with d=%o,for iteration number %o
we have the following upper bound for the primes p,
by LMN results, %o, with K=%o,km:=%o L=%o,
rho=%o,h=%o,k:=%o \n\n", D, P, d, i, B2,K,km,L,r,h,k;
i:=i+1;
end while;
end if;
if (n eq 3) then
i:=1;
B2:=7;
while B2 lt B do
if B2 gt 7 then
B:=B2;
end if;
R1,R2,R3,S1,S2,S3,T1,T2,T3,Chi,m,K,rh,L,B2,BR,BS,
BT:=LinearFormin3Logs(alpha,ha,v,hv,D1,D2,B,delta);
printf "for D=%o, with signature (d1,d2)=%o, with d=%o,
 we have the following upper bound for the primes p,
 by Mignotte results and iteration %o, %o,\n with R1=%o,
 R2=%o,R3=%o, S1=%o,S2=%o,S3=%o, T1=%o,T2=%o,
 T3=%o, K=%o,L=%o, rho=%o, m=%o and chi=%o \n
 and with Br=%o, BS=%o and BT=%o\n\n", D, P, d,i,
 B2,R1,R2,R3,S1,S2,S3,T1,T2,T3,K,L,rh,m,Chi,
```

```
 BR,BS,BT;
i:=i+1;
end while;
end if;
end if;
end for;
else
C:=10^8;
printf "for D=%o, with signature (d1,d2):=%o, with d:=%o,
we have the following upper bound for the primes p,
by Matveev Theorem, %o\n\n ",D,P,d,C;
end if;
end for;
end for;
end for;
```

Bibliography

[Apé60a] R. Apéry. Sur une équation diophantienne. *C. Rend. Acad. Sci. paris*, 251:1263–1264, 1960.

[Apé60b] R. Apéry. Sur une équation diophantienne. *C. Rend. Acad. Sci. paris*, 251:1451–1452, 1960.

[BCDT01] C. Breuil, B. Conrad, F. Diamond, and R. L. Taylor. On the modularity of elliptic curves over $\mathbb{Q}$: wild 3-adic exercises. *J. Amer. Math. Soc.*, 14:843–939, 2001.

[Beu81] F. Beukers. On the generalized Ramanujan-Nagell equation I. *Acta Arith.*, 38:389–410, 1981.

[BH96] Y. Bilu and G. Hanrot. Solving Thue Equations of High Degree. *J. Number Theory*, 60:373–392, 1996.

[Bla76] J. Blass. A note on diophantine equation $Y^2 + k = X^5$. *Math. Comp.*, 30:638–640, 1976.

[BMS06] Y. Bugeuad, M. Mignotte, and S. Siksek. Classical and modular approaches to exponential Diophantine equations II. the Lesbegue-Naguell equation. *Composotio Math.*, 142:31–62, 2006.

[BMS+08] Y. Bugeuad, M. Mignotte, S. Siksek, M. Stoll, and S. Tengely. Integral points on hyperelliptic curves. *Algebra Number Theory*, 2(8):859–885, 2008.

[BS78] J. Blass and R. Steiner. On the equation $y^2 + k = x^7$. *Utilitas Math.*, 13:293–297, 1978.

[BS01] Y. Bugeuad and T. N. Shorey. On the number of solutions of the generalized Ramanujan-Nagell equation. *I. J. reine angew. Math.*, 539:55–74, 2001.

[BS04] M. A. Bennett and C. M. Skinner. Ternary Diophantine equations via Galois representations and Modular Forms. *Canad. J. math.*, 56:23–54, 2004.

[BS08] N. Bruin and M. Stoll. Deciding existence of rational points on curves: an experiment. *Experiment. Math.*, 17(2):181–189, 2008.

[BVY04] M. A. Bennett, V. Vatsal, and S. Yazdani. Ternary Diophantine Equations of Signature $(p, p, 3)$. *Composotio Mathematica*, 140:1399–1416, 2004.

[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] J. H. E. Cohn. The Diophantine equation $x^2 + C = y^n$. *Acta Arith.*, 55:367–381, 1993.

[Coh00] Henri Cohen. *A Course in Computational Algebraic Number Theory*, volume 138. Springer-Verlag, 2000.

[Coh07a] Henri Cohen. *Number Theory Volume I: Tools and Diophantine Equations*, volume 239. Springer-Verlag, 2007.

[Coh07b] Henri Cohen. *Number Theory Volume II: Analytic and Modern tools*, volume 240. Springer-Verlag, 2007.

[Cre96] J. E. Cremona. *Algorithms for modular elliptic curves*. Cambridge University Press, second edition, 1996.

[CS03] J. E. Cremona and S Siksek. On the diophantine equation $x^2+7 = y^m$. *Acta Arith.*, 109:143–149, 2003.

[Dah08] S. R. Dahmen. *Classical and Modular Methods Applied to Diophantine Equations*. PhD thesis, Universeit Utrecht, 2008.

[DK95] J. Diamond and K. Kramer. Modularity of a family of elliptic curves. *Math. Res. lett.*, 2:299–304, 1995.

[DS05] F. Diamond and J. Shurman. *A first course in modular forms*, volume 228 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2005.

[Eul70] L. Euler. *Vollständige Einleitung zur Algebra*, volume 2 of *Unter Mitwirkung von Joh. Niessner in revidierter Fassung neu herausgegeben von Jos. E. Hofmann*. Reclam-Verlag, Stuttgart, 1770.

[Fre86] G. Frey. Links between stable elliptic curves and certain diophantine equations. *Ann. Univ. Sarav., Ser Math.*, 1:1–40, 1986.

[GPZ94] J. Gebel, A. Pethő, and H. G. Zimmer. Computing integral points on elliptic curves. *Acta. Arith.*, 68:171–192, 1994.

[GPZ98] J. Gebel, A. Pethő, and H. G. Zimmer. On Mordell's equation. *Compositio Math.*, 110:335–367, 1998.

[Han00] G. Hanrot. Solving Thue Equations without the full Unit group. *Math. Comp.*, 69(229):395–305, 2000.

[Hel72] Y. Hellegouarch. Courbes elliptiques et équation de Fermat. http://www.math.unicaen.fr/ nitaj/hellegouarch.html, 1972.

[Hem54] Ove Hemer. Notes on the diophantine equation $y^2 - k = x^3$. *Ark. Mat.*, 3:67–77, 1954.

[IK06] W. Ivorra and A. Kraus. Quelques résultats sur les équations $ax^p + by^p = cz^2$. *Canad. J. math.*, 58:115–153, 2006.

[IR82] K. Ireland and M. Rosen. *A Classical Introduction to Modern Number Theory*, volume 84. Springer-Verlag, second edition, 1982.

[Ivo03] W. Ivorra. Sur les équations $x^p + 2^\beta y^p = z^2$ et $x^p + 2^\beta y^p = 2z^2$. *Acta Arith.*, 108:327–338, 2003.

[Ko64] Chao Ko. On the diophantine equation $x^2 = y^n + 1, xy \neq 0$. *Sci. Sinica (Notes)*, 14:457–460, 1964.

[KO92] A. Kraus and J Oesterlé. Sur une question de B. Mazur. *Math. Ann.*, 293:259–275, 1992.

[Kra97] A. Kraus. Majorations effectives pour l'équation de Fermat généraisée. *Canad. J. math.*, 49:1139–1161, 1997.

[Kra98] A. Kraus. Sur l'équation $a^3 + b^3 = c^p$. *Experiment. Math.*, 7:1–13, 1998.

[Lau08] M. Laurent. Linear forms in two logarithms and interpolation determinats II. *Acta Arith.*, 133(4):325–348, 2008.

[Leb50] V. A. Lebesgue. Sur l'impossibilité en nombres entiers de l'équation $x^m = y^2 + 1$. *Nouvelles Annales des Mathématiques*, 9(1):178–181, 1850.

[Les98] J.-L. Lesage. Différence entre puissances et carrés d'entiers. *J. of Number Theory*, 73:390–425, 1998.

[Lju43] W. Ljunggren. Űber einige Arcustagensgleichungen die auf interessante unbestimmte Gleichungen fűhren. *Ark. Mat. Astr. Rys.*, 29A(13), 1943.

[LMN95] M. Laurent, M. Mignotte, and Yu. Nesterenko. Formes linéaires en deux logarithmes et déterminants d'interpolation. *J. Number Theory*, 55:255–265, 1995.

[Mat00] E. M. Matveev. An explicit lower bound for a homogeneous rational linear form in the logarithms of algebraic numbers. II. *Izvestiya Mathematics*, 64(6):1217–1269, 2000.

[MdW96] M. Mignotte and B. M. M. de Weger. On the equations $x^2 + 74 = y^5$ and $x^2 + 86 = y^5$. *Glasgow Math. J.*, 38(1):77–85, 1996.

[Mig84] M. Mignotte. Une nouvele résolution de l'équation $x^2 + 7 = 2^n$. *Sem. Rend. Fac. sc. Cagliari*, 54.2:41–43, 1984.

[Mig08] M. Mignotte. A kit on linear forms in three logarithms. *Publ. IRMA, Strasbourg, to appear*, 2008.

[Mil06] J. S. Milne. *Elliptic Curves*. BookSurge Publishing, 2006.

[Miy06] T. Miyake. *Modular forms*. Springer Monographs in Mathematics. Springer-Verlag, Berlin, english edition, 2006.

[Mor69] L. J. Mordell. *Diophantine Equations*, volume 30. Academic Press, 1969.

[Nag48] T. Nagell. Løsning til oppgave nr 2, 1943, s. 29. *Nordisk Mat. Tidskr.*, 30:62–64, 1948.

[Nag54] T. Nagell. Verallgeminerung eines Fermatschen Satzes. *Arch. Math. (Basel)*, 5:153–159, 1954.

[Nag02] T. Nagell. Collected papers of Trygve Nagell. *Queen's Papers in Pure and Applied Mathematics*, 1-4(121), 2002.

[Pap93] I. Papadopoulos. Sur la classification de Néron des courbes elliptiques en caractérisque résiduelle 2 et 3. *Journal of Number Theory*, 44:192–152, 1993.

[Ram13] S. Ramanujan. Question 464. *J. Indian Math. Soc.*, 5:120, 1913.

[Rib90] K. Ribet. On the modular representations of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. *Invent. Math.*, 100:431–476, 1990.

[Ros95] H. E. Rose. *A course in Number Theory*. Oxford Science Publications, 1995.

[Ser87] J.-P. Serre. Sur les représentations modulaires de degré 2 de $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. *Duke Math. J.*, 54:179–230, 1987.

[Shi94] G. Shimura. *Introduction to the arithmetic theory of automorphic functions*, volume 11 of *Publications of the Mathematical Society of Japan*. Princeton University Press, Princeton, NJ, 1994.

[Sho06] T. N. Shorey. Diophantine approximations, Diophantine equations, Transcendence and Applications. *Indian Jour. of Pure and Applied Math.*, 37(1):9–39, 2006.

[Sik03] S. Siksek. On the diophantine equation $x^2 = y^p + 2^k z^p$. *J. Théor. Nombres Bordeaux*, 15:839–846, 2003.

[Sikar] S. Siksek. The modular approach to Diophantine equations. In *Explicit Methods in Number Theory*. Panoramas et Synthèses (Société Mathématique de France), to appear.

[Sil85] J. H. Silverman. *The arithmetic of elliptic curves*, volume 106. Springer-Verlag, 1985.

[Sil94] J. H. Silverman. *Advanced topics in the arithmetic of elliptic curves*, volume 151. Springer-Verlag, 1994.

[Sma98] Nigel P. Smart. *The Algorithmic Resolution of Diophantine Equations*, volume 41. London Mathematical Society Student Texts, 1998.

[SS08] N. Saradha and A. Srinivasan. Generalized Lebesgue-Ramanujan-Nagell Equations. In N. Saradha, editor, *Diophantine Equations*, pages 207–223. Tata Institute of Fundamental Research Studies in Mathematics, 20., 2008.

[ST87] I. N. Stewart and D. O. Tall. *Algebraic Number Theory*. Chapman & Hall, second edition, 1987.

[Sto98] M. Stoll. On the arithmetic of the curves $y^2 = x^l + A$ and their Jacobians. *J. reine angew. Math.*, 501:171–189, 1998.

[Sto02] M. Stoll. On the arithmetic of the curves $y^2 = x^l + A$, II. *J. Number Theory*, 93:183–206, 2002.

[Sto06] M. Stoll. On the number of rational squares at fixed distance from a fifth power. *Acta Arith.*, 125:79–88, 2006.

[Tat75] J. Tate. Algorithm for determining the type of a singular fiber in an elliptic pencil. In *Modular functions of one variable, IV (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972)*, pages 33–52. Lecture Notes in Math., Vol. 476. Springer, Berlin, 1975.

[TW95] R. L. Taylor and A. Wiles. Ring thoeretic properties of certain hecke algebras. *Annals of Math.*, 141:553–572, 1995.

[Wil95] A. Wiles. Modular elliptic curves and Fermat's Last Theorem. *Annals of Math.*, 141:443–551, 1995.

[Wre73] B. M. E. Wren. $y^2 + D = x^5$. *Eureka*, 36:37–38, 1973.