Solvability of ternary equations of signature \((3, 3, 2)\)

by

Patrick Ryan McMahon

B.Sc. (Hons), University of British Columbia, 2011

A THESIS SUBMITTED IN PARTIAL FULFILLMENT
OF THE REQUIREMENTS FOR THE DEGREE OF

Master of Science

in the

Department of Mathematics
Faculty of Science

© Patrick Ryan McMahon 2014

SIMON FRASER UNIVERSITY
Summer 2014

All rights reserved.
However, in accordance with the Copyright Act of Canada, this work may be
reproduced without authorization under the conditions for “Fair Dealing.”
Therefore, limited reproduction of this work for the purposes of private study,
research, criticism, review and news reporting is likely to be in accordance
with the law, particularly if cited appropriately.
APPROVAL

Name: Patrick Ryan McMahon
Degree: Master of Science
Title of Thesis: Solvability of ternary equations of signature (3, 3, 2)

Examiner Committee: 
Dr. Petr Lisonek
Chair

Dr. Nils Bruin
Associate Professor of Mathematics
Simon Fraser University
Senior Supervisor

Dr. Michael Monagan
Professor of Mathematics
Simon Fraser University
Supervisor

Dr. Stephen Choi
Professor of Mathematics
Simon Fraser University
Internal Examiner

Date Approved: August 11th, 2014
Partial Copyright Licence

The author, whose copyright is declared on the title page of this work, has granted to Simon Fraser University the non-exclusive, royalty-free right to include a digital copy of this thesis, project or extended essay[s] and associated supplemental files (“Work”) (title[s] below) in Summit, the Institutional Research Repository at SFU. SFU may also make copies of the Work for purposes of a scholarly or research nature; for users of the SFU Library; or in response to a request from another library, or educational institution, on SFU’s own behalf or for one of its users. Distribution may be in any form.

The author has further agreed that SFU may keep more than one copy of the Work for purposes of back-up and security; and that SFU may, without changing the content, translate, if technically possible, the Work to any medium or format for the purpose of preserving the Work and facilitating the exercise of SFU’s rights under this licence.

It is understood that copying, publication, or public performance of the Work for commercial purposes shall not be allowed without the author’s written permission.

While granting the above uses to SFU, the author retains copyright ownership and moral rights in the Work, and may deal with the copyright in the Work in any way consistent with the terms of this licence, including the right to change the Work for subsequent purposes, including editing and publishing the Work in whole or in part, and licensing the content to other parties as the author may desire.

The author represents and warrants that he/she has the right to grant the rights contained in this licence and that the Work does not, to the best of the author’s knowledge, infringe upon anyone’s copyright. The author has obtained written copyright permission, where required, for the use of any third-party copyrighted material contained in the Work. The author represents and warrants that the Work is his/her own original work and that he/she has not previously assigned or relinquished the rights conferred in this licence.

Simon Fraser University Library
Burnaby, British Columbia, Canada

revised Fall 2013
Abstract

In this thesis we examine the primitive solvability of Diophantine equations of the form $ax^3 + by^3 = cz^2$. For square-free $a, b, c$, we identify various criteria necessary for the existence of primitive solutions, including a sufficient one. We also present a relatively efficient algorithm to determine whether this criterion is satisfied. Using the algorithm, we compute some data on the relative distribution of the occurrence of various obstructions to the existence of primitive solutions.
Acknowledgments

I would like to thank my family and friends, whose constant support and encouragement have made my accomplishments possible. I would also like to thank Lindsay, for her love and patience while I have completed this degree. I especially want to thank my supervisor, Nils, for his comments, criticism and for all the support that he has given me. Lastly, I wish to thank all the staff in the SFU Mathematics Department for providing such a great environment for research and study.
## Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Approval</td>
<td>ii</td>
</tr>
<tr>
<td>Partial Copyright License</td>
<td>iii</td>
</tr>
<tr>
<td>Abstract</td>
<td>iv</td>
</tr>
<tr>
<td>Acknowledgments</td>
<td>v</td>
</tr>
<tr>
<td>Contents</td>
<td>vi</td>
</tr>
<tr>
<td>List of Tables</td>
<td>viii</td>
</tr>
<tr>
<td>List of Figures</td>
<td>ix</td>
</tr>
<tr>
<td><strong>1 Introduction</strong></td>
<td>1</td>
</tr>
<tr>
<td>1.1 The generalized Fermat equation</td>
<td>2</td>
</tr>
<tr>
<td><strong>2 Background</strong></td>
<td>6</td>
</tr>
<tr>
<td>2.1 The ideal class group</td>
<td>6</td>
</tr>
<tr>
<td>2.2 $p$-adic numbers</td>
<td>15</td>
</tr>
<tr>
<td><strong>3 Solving $ax^3 + by^3 = cz^2$</strong></td>
<td>17</td>
</tr>
<tr>
<td>3.1 Local obstructions</td>
<td>18</td>
</tr>
<tr>
<td>3.2 Class group obstructions</td>
<td>18</td>
</tr>
<tr>
<td>3.3 Parametrizing $ax^3 + by^3 = cz^2$</td>
<td>23</td>
</tr>
<tr>
<td>3.4 Covering obstructions</td>
<td>28</td>
</tr>
</tbody>
</table>
4 Computational approach

4.1 Outline ........................................................................ 36
4.2 Computing \( \mu(D_p) \) .................................................. 42
4.3 Computing Sel\((D(k))\) .................................................. 47
4.4 Results ........................................................................ 48

Bibliography ...................................................................... 52

Appendix A Equivalent \( ax^3 + by^3 = cz^2 \) ...................... 54

Appendix B Data tables ....................................................... 55

Appendix C MAGMA Code ............................................... 57
List of Tables

4.1 Random sample data for $D(a,b,c)$ when $\#\text{Cl}(K)$ is even ............... 51
4.2 Random sample data for $D(a,b,c)$ when $\#\text{Cl}(K)$ is odd ............... 51

B.1 Statistics for $D(a,b,c)$ ......................................................... 55
B.2 Statistics for $D(a,b,c)$ when $\#\text{Cl}(K)$ is even ....................... 56
B.3 Statistics for $D(a,b,c)$ when $\#\text{Cl}(K)$ is odd ....................... 56
List of Figures

4.1 Proportion chart of obstructions, $b, c \leq H$, $H = 20, \ldots, 3000$ . . . . . . . . . . . 49
4.2 Proportion chart of obstructions, $\#\text{Cl}(K)$ even, $b, c \leq H$, $H = 20, \ldots, 3000$ . 50
4.3 Proportion chart of obstructions, $\#\text{Cl}(K)$ odd, $b, c \leq H$, $H = 20, \ldots, 3000$ . 51
Chapter 1

Introduction

Diophantine equations have been studied since antiquity and their subject is one of the oldest branches of mathematical inquiry. Named in recognition of the 3rd century hellenistic mathematician Diophantus of Alexandria, whose *Arithmetica* contains some of the earliest usage of symbols in algebra, these eponymous equations have both vexed and intrigued mathematicians for centuries.

In the 17th century, Pierre de Fermat, working through a copy of *Arithmetica*, came across the Pythagorean equation and, generalizing it, claimed that for any \( n > 2 \), the equation \( x^n + y^n = z^n \) has no positive integer solutions. Claiming to have found a marvellous proof of this proposition, Fermat left posterity with only a note to this effect, thereby leaving mathematics with a conjecture that would remain unsolved for over 350 years.

Mathematics would have to wait until 1994 and Wiles’ famous proof of the modularity theorem to see Fermat’s conjecture fully resolved. Due to its stubbornness, efforts to solve Fermat’s famous problem have led to the development of many interesting and useful areas of mathematics.

Soon after this celebrated development, broader research began on generalizations of Fermat’s equation. This thesis continues in this tradition by studying equations of the form

\[ ax^3 + by^3 = cz^2. \]
We present several necessary conditions for \(ax^3 + by^3 = cz^2\) to have primitive (relatively prime) solutions and show how, when they exist, solutions are obtained. In the final chapter we discuss a necessary and sufficient criterion for the existence of primitive solutions to this equation and describe a computational procedure for determining whether this criterion is met. We conclude by presenting some statistics obtained by our implementation of the algorithm.

### 1.1 The generalized Fermat equation

A **generalized Fermat equation** is a ternary equation of the form

\[
ax^p + by^q = cz^r
\]  

(1.1)

where \(p, q, r \in \mathbb{Z}_{\geq 2}\) and \(a, b, c\) are nonzero integers. The **signature** of an equation of this form is the triple \((p, q, r)\) and here we are interested in primitive solutions, that is \((x, y, z) \in \mathbb{Z}^3\) with \(\gcd(x, y, z) = 1\).

The main characteristics of (1.1) are determined by the value of

\[
\chi = 1/p + 1/q + 1/r.
\]

If \(\chi = 1\), then \((p, q, r)\) must be one of \((3, 3, 3), (2, 3, 6)\) or \((4, 4, 2)\). This is called the **Euclidean case**. Here, primitive solutions correspond to rational points on finitely many algebraic curves of genus 1. Depending on the curves, there will be zero, finitely many or infinitely many solutions [13].

If \(\chi < 1\), the **hyperbolic case**, then there is also a finite set of parametrizing curves, however in this case the curves are of genus \(> 1\). Using Faltings’ theorem, Darmon and Granville were able to show that in this case there are only finitely many solutions:

**Theorem 1.1.1 (Darmon, Granville).** Let \(a, b, c \in \mathbb{Z}, abc \neq 0\) and \(p, q, r \in \mathbb{Z}_{\geq 2}\) such that \(\chi < 1\). The equation \(ax^p + by^q = cz^r\) has only finitely many solutions with \(x, y, z \in \mathbb{Z}\) and \(\gcd(x, y, z) = 1\). [6]

If \(\chi > 1\), then \((p, q, r)\) must be one of \((2, 3, 3), (2, 3, 4), (2, 3, 5)\) or \((2, 2, m)\) where \(m \geq 2\). We
call this the spherical case. It has been shown that there exists a finite set of polynomial solutions such that the integral solutions can be obtained by specializing:

**Theorem 1.1.2 (Beukers).** Let $a, b, c \in \mathbb{Z}$ with $abc \neq 0$ and $p, q, r \in \mathbb{Z}_{\geq 2}$ such that $\chi > 1$. Then the equation $ax^p + by^q = cz^r$ has either zero or infinitely many solutions $(x, y, z)$ in $\mathbb{Z}$ with $\gcd(x, y, z) = 1$. Moreover, there is a finite set of triples $X, Y, Z \in \mathbb{Q}[U, V]$ with $\gcd(X, Y, Z) = 1$ and $aX^p + bY^q = cZ^r$ such that for every primitive integral solution $(x, y, z)$, for one of these triples $(X, Y, Z)$ there are $u, v \in \mathbb{Q}$ such that $x = X(u, v), y = Y(u, v)$ and $z = Z(u, v)$. [1]

The class of equations that we consider in this thesis falls under the spherical case. We briefly present some results from the literature for the standard (i.e. $a = b = c = 1$) cases.

The equation $x^2 + y^3 = z^3$ where $\gcd(x, y, z) = 1$ was originally solved in full by Mordell in [11].

The equation $x^2 + y^3 = z^4$ where $\gcd(x, y, z) = 1$ was solved by Zagier and the results presented by Beukers in [1].

The equation $x^2 + y^3 = z^5$ where $\gcd(x, y, z) = 1$ was solved by Edwards in [7].

Edwards’ approach to solving the hitherto inaccessible $(2, 3, 5)$ case uses classical invariant theory and Klein forms and is also able to solve $(2, 3, 3)$ and $(2, 3, 4)$. His approach reduces the determination of the parametrizations in Theorem 1.1.2 to a finite procedure by showing that all of the required parametrizations can be obtained from integers $a_0, a_1, a_2$ less than some bound which is polynomial in the coefficients $a, b, c$; See [7, Chapter 11]. His method is then to consider all possible $a_0, a_1, a_2$ in this box, and analyze the parametrizations obtained from them. This algorithm is fully exponential in the bit lengths of $a, b, c$.

We provide an alternative approach which splits up the computations per prime divisor of $6abc$. The algorithm given in Section 4.2 depends badly on the size of these primes, since part of the algorithm involves iterating over representatives of $\mathbb{F}_p$. However, if $6abc$ is large but consists of many small primes, then the total time expended here compares
quite favourably. An additional bottleneck in our procedure is that we need to compute the class group of the number field $\mathbb{Q}(\sqrt[3]{b/a})$. Without assuming the Generalized Riemann Hypothesis, this requires computation time exponential in $\log(ab)$ but doing this is practical with standard software for large ranges.

**Remark.** Since we allow both positive and negative coefficients, solving equations with signature $(3,3,2)$ is equivalent to solving equations with signature $(2,3,3)$. This follows from the fact that, for equations of signature $(3,3,2)$, only one of $p,q,r$ is even and hence we can absorb negative signs into the cubic powers.

In the spherical case, we know by Theorem 1.2.1 that if there exist any primitive solutions to (1.1), then there are infinitely many and that there exists a finite set of parametrizations such that every solution can be obtained by specializing. While Beukers’ theory gives us complete information regarding the size of the solution set, it does not provide a feasible method of obtaining the parametrizations.

A technique which often provides an effective way to obtain the parametrizations for some spherical equations can be seen in the following solution of the Pythagorean triples.

**Proposition 1.1.3.** The primitive solutions of the equation $x^2 + y^2 = z^2$ are given by the parametrizations

\[
\begin{align*}
x &= s^2 - t^2 \\
y &= 2st \\
z &= \pm(s^2 + t^2)
\end{align*}
\]

up to interchanging $x$ and $y$.

**Proof.** Suppose that $(x,y,z)$ is a primitive integral solution of $x^2 + y^2 = z^2$. Considering $x,y,z \mod 4$ we find that $z$ and one of $x,y$ must be odd and using the symmetry of the equation we assume that $x$ is odd and $y$ even. Factoring over $\mathbb{Z}[i]$ we obtain

\[(x + iy)(x - iy) = z^2\]

We claim that $(x + iy) = \epsilon z_1^2$ for some unit $\epsilon$ and arbitrary $z_1 \in \mathbb{Z}[i]$. To see this, note that any common factor of $x + iy$ and $x - iy$ must also divide $2x$ and $2iy$ and therefore must
divide $2 = (1 + i)(1 - i)$. But this would imply that $2 \mid z^2$, contradicting the parity of $z$. Hence $x + iy$ has no common factor with $x - iy$ and therefore the claim must hold as $\mathbb{Z}[i]$ is a Euclidean domain. Write $z_1 = s + it$ for some integers $s, t$, then we have

$$(x + iy) = \epsilon(s + it)^2 = \epsilon(s^2 + 2ist - t^2)$$

where $\epsilon \in \{1, -1, i, -i\}$. Considering each $\epsilon$ and comparing coefficients yields the result. □

This is a classical proof and although the method is by no means the only way to obtain the parametrizing curves, it does extend well to the case where $(p, q, r) = (3, 3, 2)$. In the next chapter we cover the theory required to describe effective methods for deciding primitive solvability of these equations.
Chapter 2

Background

2.1 The ideal class group

We start with some basic definitions and results from algebraic number theory. An algebraic number field (sometimes just called number field) $K$ is a finite field extension of $\mathbb{Q}$ and elements of $K$ are called algebraic numbers. An algebraic number is said to be integral if it is a root of some monic polynomial in $\mathbb{Z}[x]$. The degree of $K$, denoted $[K : \mathbb{Q}]$, is the dimension of $K$ as a vector space over $\mathbb{Q}$. An elementary result for number fields gives that any number field $K/\mathbb{Q}$ is of the form $K = \mathbb{Q}(\alpha)$ for some $\alpha \in K$, where $\alpha$ is integral. Moreover, $K = \mathbb{Q}(\alpha) = \mathbb{Q}[x]/(f(x))$, where $f(x)$ is square-free in $\mathbb{Q}[x]$. In particular, this means that number fields always meet a certain technical condition: they are always separable.

Definition 2.1.1. Let $A \subseteq B$ be an extension of rings. An element $b \in B$ is called integral over $A$, if it satisfies a monic equation

$$x^n + a_1x^{n-1} + \cdots + a_n = 0, \quad n \geq 1,$$

with coefficients $a_i$ in $A$. The ring $B$ is called integral over $A$ if all elements $b \in B$ are integral over $A$. 
Proposition 2.1.2. [12, Proposition 2.2] If $A \subseteq B$ is an extension of rings then the set of all elements

$$A^{ic} = \{b \in B \mid b \text{ integral over } A\}$$

forms a ring. We call this ring the integral closure of $A$ in $B$. The ring $A$ is said to be integrally closed in $B$ if $A = A^{ic}$.

We now consider a more specialized situation. Let $A$ be an integral domain which is integrally closed in $K$ its field of fractions, $L/K$ a finite field extension, and $B$ the integral closure of $A$ in $L$. Then, by the previous proposition, $B$ is integrally closed automatically and furthermore the fact that $A$ is integrally closed means that any element $\beta \in L$ is integral over $A$ if and only if its minimal polynomial $p(x)$ takes coefficients in $A$.

Next we introduce the trace and norm in a field extension $L/K$, which are important tools for the study of integral elements in $L$. We define these as follows

Definition 2.1.3. The trace and norm of an element $x \in L$ are defined to be the trace and determinant, respectively, of the endomorphism

$$T_x : L \rightarrow L, \quad T_x(\alpha) = x\alpha$$

of the $K$-vector space $L$:

$$\text{Tr}_{L/K}(x) = \text{Tr}(T_x), \quad \text{N}_{L/K}(x) = \det(T_x)$$

Now, $T_{x+y} = T_x + T_y$ and $T_{xy} = T_x \circ T_y$, so that $\text{Tr}_{L/K}$ and $\text{N}_{L/K}$ define homomorphisms

$$\text{Tr}_{L/K} : L \rightarrow K, \quad \text{N}_{L/K} : L^* \rightarrow K^*$$

on the additive and multiplicative subgroups, respectively, of $L$. In the case where the extension $L/K$ is separable, the trace and norm admit the following Galois-theoretic interpretation.
**Proposition 2.1.4.** [12, Proposition 2.6] If $L/K$ is a separable extension and $\sigma : L \to \overline{K}$ varies over the different $K$ embeddings of $L$ into an algebraic closure $\overline{K}$ of $K$, then we have

\begin{align*}
(i) \quad \text{Tr}_{L/K}(x) &= \sum_{\sigma} \sigma x \\
(ii) \quad N_{L/K}(x) &= \prod_{\sigma} \sigma x
\end{align*}

We return to an integrally closed integral domain $A$ with field of fractions $K$ and integral closure $B$ in some finite separable extension $L/K$. If $x \in B$ is an integral element of $L$, then all of its conjugates $\sigma x$ are also integral. Furthermore

$$\text{Tr}_{L/K}(x), \ N_{L/K}(x) \in A$$

A system of elements $\omega_1, \ldots, \omega_n \in B$ such that each $b \in B$ can be written uniquely as

$$b = a_1 \omega_1 + \cdots + a_n \omega_n$$

with $a_i \in A$, is called an **integral basis** of $B$ over $A$. Such an integral basis is automatically also a basis for $L/K$ and therefore its length, $n$, must equal the degree of the field extension $[L : K]$. The fact that $B$ lies inside a finite field extension $L$ of the field of fractions $K$ of $A$ provides us with some additional structure on $B$. First of all $B$ is closed with respect to addition and scaler multiplication by $A$, making $B$ into an $A$-module. The following result guarantees that, as an $A$-module, $B$ looks like $A^{[L : K]}$, i.e. that an integral basis for $B$ exists.

**Proposition 2.1.5.** [12, Proposition 2.10] If $L/K$ is separable and $A$ is a principal ideal domain, then every finitely generated $B$-submodule $M \neq 0$ of $L$ is a free $A$-module of rank $[L : K]$. In particular, $B$ admits and integral basis over $A$.

The main application of these considerations on integrality will concern the integral closure $\mathcal{O}_K \subseteq K$ of $\mathbb{Z} \subseteq \mathbb{Q}$ in an algebraic number field $K$.

**Definition 2.1.6.** The **ring of integers** of a number field $K$, denoted $\mathcal{O}_K$, is the integral closure of $\mathbb{Z}$ in $K$.

The ring of integers generalizes the role played by the rational integers. Like with $\mathbb{Z}$, every non-unit can be factored in $\mathcal{O}_K$ into a product of irreducible elements, however unlike with $\mathbb{Z}$ this decomposition into a product of irreducible elements is not necessarily unique (up to
associate). As we shall soon see, while unique factorization may not hold for elements in $O_K$, we do have unique factorization for the ideals of $O_K$. We now make this distinction more clear.

**Theorem 2.1.7.** [12, Theorem 3.1] The ring $O_K$ is noetherian, integrally closed, and every prime ideal $p \neq 0$ is maximal.

**Definition 2.1.8.** A noetherian, integrally closed integral domain in which every nonzero prime ideal is maximal is called a **Dedekind domain**.

In the same way that rings of the form $O_K$ can be viewed as generalizations of $\mathbb{Z}$, Dedekind domains can be thought of as generalized principal ideal domains.

In the subsequent pages we provide the necessary background needed to begin making statements about prime ideal factorization in $O_K$.

Let $O$ be a Dedekind domain. Given two ideals $a$ and $b$ of $O$, the divisibility relation $a \mid b$ is defined by $b \subseteq a$, and the sum of the ideals by

$$a + b = \{a + b \mid a \in a, b \in b\}.$$ 

This is the smallest ideal containing $a$ as well as $b$, which we can think of as the greatest common divisor of $a$ and $b$. Similarly, the intersection of two ideals $a \cap b$ can be thought of as the least common multiple of $a$ and $b$. Lastly, we define the product of $a$ and $b$ as

$$ab = \left\{ \sum_{i=1}^{d} a_i b_i \mid a_i, b_i \in a, b, d < \infty \right\}.$$ 

With respect to this multiplication, the ideals of $O$ will grant us the property that the elements alone may fail to provide, **unique prime factorization**.

**Theorem 2.1.9.** [12, Theorem 3.3] Every ideal $a$ of $O$ different from $(0)$ and $O$ admits a factorization

$$a = p_1 \cdots p_r$$

into nonzero prime ideals $p_i$ of $O$ which is unique up to the order of the factors.

Now, with $O$ still a Dedekind domain, we may obtain **inverses** for the nonzero ideals of $O$ by introducing the notion of a fractional ideals in the field of fractions $K$. 
Definition 2.1.10. A fractional ideal of $K$ is a finitely generated $\mathcal{O}$-submodule $a \neq 0$ of $K$.

For example, every $a \in K^*$ defines the fractional “principal ideal” $(a) = a\mathcal{O}$. Also, since $\mathcal{O}$ is noetherian, it is clear that an $\mathcal{O}$-submodule is a fractional ideal if and only if there exists $c \in \mathcal{O}, c \neq 0$, such that $ca \subseteq \mathcal{O}$ is an ideal of the ring $\mathcal{O}$. For distinction we shall henceforth refer to the latter as integral ideals of $K$.

Proposition 2.1.11. [12, Proposition 3.8] The fractional ideals form an abelian group, the ideal group $J_K$ of $K$. The identity element is $(1) = \mathcal{O}$ and the inverse of $a$ is

$$a^{-1} = \{x \in K \mid xa \subseteq \mathcal{O}\}.$$

Corollary 2.1.12. [12, Corollary 3.9] Every fractional ideal $a$ admits a unique representation as a product

$$a = \prod_p p^{\nu_p}$$

with $\nu_p \in \mathbb{Z}$ and $\nu_p = 0$ for almost all $p$. In other words, $J_K$ is the free abelian group on the set of nonzero prime ideals $p$ of $\mathcal{O}$.

The fractional principal ideals $(a) = a\mathcal{O}, a \in K^*$, form a subgroup of the ideal group $J_K$ which will be denoted $P_K$. The quotient group

$$\text{Cl}(K) = J_K/P_K$$

is called the ideal class group, or class group for short, of $K$. For general Dedekind domains, we can say very little about the structure of the abelian group $\text{Cl}(K)$, however for the ring of integers $\mathcal{O}_K$ in a number field $K$ one obtains important finiteness theorems. First though, we introduce the notion of the norm of an ideal. If $a$ is an ideal in $\mathcal{O}_K$, we define its absolute norm as the index of $a$ in $\mathcal{O}_K$ as abelian groups,

$$\mathfrak{N}(a) = [\mathcal{O}_K : a].$$

This index is always finite and the name is justified by the special case where $a$ is a principal ideal $(\alpha)$ of $\mathcal{O}_K$, in which case

$$\mathfrak{N}(a) = |N_{K/\mathbb{Q}}(\alpha)|.$$
Proposition 2.1.13. [12, Proposition 6.1] If $a = p_1^{\nu_1} \cdots p_r^{\nu_r}$ is the prime factorization of an ideal $a \neq 0$, then one has
\[ \mathfrak{N}(a) = \mathfrak{N}(p_1)^{\nu_1} \cdots \mathfrak{N}(p_r)^{\nu_r}. \]

Theorem 2.1.14. [12, Theorem 6.3] The ideal class group $\Cl(K) = J_K/P_K$ is finite. Its order
\[ h_K = [J_K : P_K] \]
is called the class number of $K$.

When $h_K = 1$, we have that $\mathcal{O}_K$ is a principal ideal domain, as we must have $J_K = P_K$. In this sense, the magnitude of the class group measures how far $\mathcal{O}_K$ is from being a PID.

After looking at the ideal class group, we now consider its group of units $\mathcal{O}_K^\times$. It contains the finite group $\mu(K)$ of the roots of unity which lie in $K$, but in general $\mathcal{O}_K^\times$ is itself not finite. Letting $r$ denote the number of real embeddings $\rho : K \to \mathbb{C}$ and $s$ the number of pairs of complete conjugate embeddings $\sigma : K \to \mathbb{C}$, we have following theorem

Theorem 2.1.15 (Dirichlet’s Unit Theorem). [12, Theorem 7.4] The group of units $\mathcal{O}_K^\times$ of $\mathcal{O}_K$ is the direct product of the finite cyclic group $\mu(K)$ and a free abelian group of rank $r + s - 1$.

In other words: there exist units, $\varepsilon_1, \ldots, \varepsilon_t$, where $t = r + s - 1$, called fundamental units, such that any other unit $\varepsilon$ can be written uniquely as
\[ \varepsilon = \zeta \varepsilon_1^{\nu_1} \cdots \varepsilon_t^{\nu_t} \]
with a root of unity $\zeta$ and integers $\nu_i$.

Henceforth we take $K$ to be a number field. For a rational prime $p \in \mathbb{Z}$ one always has
\[ p\mathcal{O}_K \neq \mathcal{O}_K. \]

Moreover, a prime ideal $p\mathbb{Z}$ of the integers decomposes in $\mathcal{O}_K$ in a unique way into a product of prime ideals
\[ p\mathcal{O}_K = p_1^{\nu_1} \cdots p_r^{\nu_r}. \]
The prime ideals $p_i$ occurring in the decomposition are precisely those prime ideals $p$ of $O_K$ which lie over $p\mathbb{Z}$ in the sense that one has the relation

$$p\mathbb{Z} = p \cap \mathbb{Z}.$$ 

We denote this for short by $p \mid (p)$, and we call $p$ a prime divisor of $(p)$. The exponent $e_i$ is called the ramification index and the degree of the field extension

$$f_i = [O_K/p_i : \mathbb{Z}/p\mathbb{Z}]$$

is called the inertia degree of $p_i$ over $p$. If the extension $K/\mathbb{Q}$ is separable, then the numbers $e_i, f_i$ and $n = [K : \mathbb{Q}]$ are connected by the following law.

**Proposition 2.1.16.** [12, Proposition 8.2] Let $K/\mathbb{Q}$ be separable, let $p$ be a rational prime and let $p_1, \ldots, p_r$ be the prime ideals of $O_K$ dividing $pO_K$. Then we have the fundamental identity

$$\sum_{i=1}^r e_i f_i = n.$$ 

The prime ideal $(p)$ is said to split completely (or to be totally split) in $K$, if in the decomposition

$$(p) = p_1^{e_1} \cdots p_r^{e_r}.$$ 

one has $r = n = [K : \mathbb{Q}]$, so that $e_i = f_i = 1$ for $i = 1, \ldots, r$. The ideal $(p)$ is called nonsplit if $r = 1$, i.e., if there is only a single prime ideal of $K$ over $(p)$ and inert if additionally $e_1 = 1$. The prime ideal $p_i$ in the decomposition is called unramified over $\mathbb{Z}$ (or over $\mathbb{Q}$) if $e_i = 1$ and if the residue class field extension $O_K/p_i \mid \mathbb{Z}/p\mathbb{Z}$ is separable. If not, it is called ramified, and totally ramified if furthermore $f_i = 1$. The prime ideal $(p)$ is called unramified if all $p_i$ are unramified, otherwise it is called ramified. We have the following proposition

**Proposition 2.1.17.** [12, Proposition 8.3] Let $K = \mathbb{Q}(-\sqrt[3]{b})$, let $L = K(\theta)$ be the splitting field of $K$ and let $p$ be some prime ideal of $O_K$ such that $p$ does not lie above any prime dividing $\text{disc}(f)$ where $f = x^3 + b$. Let $p(x)$ be the minimal polynomial of $\theta$ over $K$. Let

$$\bar{p}(x) = \bar{p}_1(x)^{e_1} \cdots \bar{p}_r(x)^{e_r}$$

be the factorisation of $\bar{p}(x) \equiv p(x) \pmod{p}$ into irreducible $\bar{p}_i(x) \equiv p_i(x) \pmod{p}$ over the
residue class field $\mathcal{O}_K/p$ with all $p_i(x) \in \mathcal{O}_K[x]$ monic. Then

$$p_i = p\mathcal{O}_K + p_i(\theta)\mathcal{O}_K, \quad i = 1, \ldots, r$$

are the different prime ideals of $\mathcal{O}_L$ above $p$. The inertia degree $f_i$ is the degree of $\bar{p}_i(x)$, and one has

$$p = \mathcal{P}_1^{e_1} \cdots \mathcal{P}_r^{e_r}.$$

Next, note that we can generalize the concept of $\text{ord}_p : \mathbb{Q}^* \to \mathbb{Z}$ (defined in 3.2) in the following way.

**Definition 2.1.18.** Let $K$ be a number field and fix some prime ideal $p \subset \mathcal{O}_K$. For $\alpha \in K$, we have $\alpha \mathcal{O}_K = p^v(p_1^{e_1} \cdots p_r^{e_r})$ where $p \neq p_i$ for any $i$. We set $\text{ord}_p(\alpha) = v$.

It is straightforward to check that this is a valuation and that if $p$ is a rational prime lying below $p$ then $\text{ord}_p(p) = e_i$, where $e_i$ is the ramification index of $p$.

**Definition 2.1.19.** Let $K$ be a number field and $\mathcal{O}_K$ its ring of integers. Let $b_1, \ldots, b_n$ be an integral basis for $\mathcal{O}_K$ and let $\{\sigma_1, \ldots, \sigma_n\}$ be the set of embeddings of $K$ into the complex numbers. The discriminant of $K$ is the square of the determinant of the $n$ by $n$ matrix $B$ whose $(i,j)$'th entry is $\sigma_i(b_j)$.

**Definition 2.1.20.** Let $f \in \mathbb{Z}[x]$ be a polynomial of the form $ax^3 + b$, with $a, b \neq 0$, and let $\theta_1, \theta_2, \theta_3$ denote the roots of $f$. The discriminant of $f$ is defined as

$$\text{disc}(f) = a^4 \prod_{i \neq j} (\theta_i - \theta_j) = -27a^2b^2$$

**Proposition 2.1.21.** [12, Proposition 8.4] If $K$ is a number field, $\mathcal{O}_K$ its ring of integers and $p$ some prime ideal of $\mathcal{O}_K$ and $p$ is ramified, then $p | \Delta_K$, where $\Delta_K$ is the discriminant of $K$.

We now mention two results concerning pure cubic extensions.
Theorem 2.1.22. [5, Theorem 6.4.13] If \( K = \mathbb{Q}(\sqrt[3]{m}) \) where \( m \) is cube-free and not equal to \( \pm 1 \). Write \( m = ab^2 \) with \( a, b \) square-free and coprime. Let \( \theta \) be the cube root of \( m \) belonging to \( K \). If \( a^2 \not\equiv b^2 \pmod{9} \), then
\[
\left( 1, \theta, \frac{\theta^2}{b} \right)
\]
is an integral basis for \( \mathcal{O}_K \) and the discriminant of \( K \) is equal to \(-27a^2b^2\). If \( a^2 \equiv b^2 \pmod{9} \), then
\[
\left( 1, \theta, \frac{b^2 + ab^2\theta + \theta^2}{3b} \right)
\]
is an integral basis for \( \mathcal{O}_K \) and the discriminant of \( K \) is equal to \(-3a^2b^2\).

Remark. The rational primes dividing the discriminant of \( K = \mathbb{Q}(\sqrt[3]{m}) \) are precisely those which divide \( \text{disc}(x^3 + m) \).

Theorem 2.1.23. [5, Theorem 6.4.14] If \( K = \mathbb{Q}(\sqrt[3]{m}) \) where \( m \) is cube-free and not equal to \( \pm 1 \). Write \( m = ab^2 \) with \( a, b \) square-free and coprime. Then
\[
3\mathcal{O}_K = p^3 \quad \text{if} \quad a^2 \not\equiv b^2 \pmod{9} \\
3\mathcal{O}_K = p^2q \quad \text{if} \quad a^2 \equiv b^2 \pmod{9}
\]
with \( p \neq q \).

Lastly, we define the group \( A(2, S) \) and reference a result that guarantees its finiteness.

Definition 2.1.24. Let \( A \) be a number field and \( S \) a finite set of prime ideals of \( \mathcal{O}_A \). We define
\[
A(2, S) = \{ \delta \in A^*/A^*^2 : \text{ord}_p(\delta) \equiv 0 \pmod{2} \text{ for all } p \notin S \}
\]

Proposition 2.1.25. The group \( A(2, S) \) is finite.

Proof. See the proof of Proposition 1.6 in Chapter VIII of [14] where in Silverman’s notation \( T_S = A(2, S) \) and \( m = 2 \). \(\square\)
2.2 $p$-adic numbers

Fix a prime number $p \in \mathbb{Z}$. The $p$-adic valuation on $\mathbb{Z}$ is the function

$$\text{ord}_p : \mathbb{Z} \to \mathbb{R}$$

defined as follows: $\text{ord}_p(0) = \infty$ and for each $n \in \mathbb{Z}$, $n \neq 0$, $\text{ord}_p(n)$ is the greatest positive integer such that

$$p^{\text{ord}_p(n)} \mid n$$

We extend $\text{ord}_p$ to the rational numbers as follows: if $x = \frac{a}{b} \in \mathbb{Q}^*$, then

$$\text{ord}_p(x) = \text{ord}_p(a) - \text{ord}_p(b)$$

**Definition 2.2.1.** For any $x \in \mathbb{Q}$, we define the $p$-adic absolute value of $x$ by

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

when $x \neq 0$ and set $|0|_p = 0$.

The real numbers are obtained by completing $\mathbb{Q}$ with respect to the usual absolute value, the same construction using $p$-adic absolute value yields a complete field called the $p$-adic numbers.

**Definition 2.2.2.** The field of $p$-adic numbers, denoted by $\mathbb{Q}_p$, is the topological field obtained by completing $\mathbb{Q}$ with respect to the $p$-adic absolute value.

**Definition 2.2.3.** The ring of $p$-adic integers, denoted $\mathbb{Z}_p$ is a subset of the $p$-adic numbers defined as follows

$$\mathbb{Z}_p = \{ x \in \mathbb{Q}_p : |x|_p \leq 1 \}$$

The set of invertible elements of the $p$-adic integers forms a group called the $p$-adic units which we denote $\mathbb{Z}_p^*$. It is straightforward to verify that

$$\mathbb{Z}_p^* = \{ x \in \mathbb{Q}_p : |x|_p = 1 \}$$

and furthermore that $\mathbb{Z}_p$ has a unique maximal ideal $p\mathbb{Z}_p$. 
Proposition 2.2.4 (Hensel’s Lemma). [8, Theorem 3.4.1] Let \( f(X) = a_0 + a_1 X + \cdots + a_n X^n \) be a polynomial with coefficients in \( \mathbb{Z}_p \). Suppose that there exists a \( p \)-adic integer \( \alpha_1 \) such that
\[
f(\alpha_1) \equiv 0 \pmod{p \mathbb{Z}_p}
\]
and
\[
f'(\alpha_1) \not\equiv 0 \pmod{p \mathbb{Z}_p}
\]
where \( f'(X) \) is the derivative of \( f(X) \). Then there exists a \( p \)-adic integer \( \alpha \in \mathbb{Z}_p \) such that \( f(\alpha) = 0 \) and \( f(\alpha) \equiv f(\alpha_1) \pmod{p \mathbb{Z}_p} \).

Proposition 2.2.5. [8, Proposition 3.4.3] Let \( p \neq 2 \) be a prime and let \( b \) be a \( p \)-adic unit. If there exists \( \alpha_1 \) such that \( \alpha_1^2 \equiv b \pmod{p \mathbb{Z}_p} \), then \( b \) is the square of an element in \( \mathbb{Z}_p^* \).

Corollary 2.2.6. [8, Corollary 3.4.4] If \( p \) is odd then the quotient group \( \mathbb{Q}_p^*/(\mathbb{Q}_p^*)^2 \) has order 4.

Proposition 2.2.7. [4, Lemma 3.3] The group \( \mathbb{Q}_2^*/(\mathbb{Q}_2^*)^2 \) has order 8.

A consequence of Hensel’s Lemma is that, given a polynomial with integer coefficients, it is typically not difficult to decide whether it has roots in \( \mathbb{Z}_p \), as it usually suffices to find roots modulo \( p \). In fact, generalizations of Hensel’s Lemma show that, for a square-free polynomial, there is an explicitly computable bound \( k \) such that \( f(x) \) has roots in \( \mathbb{Z}_p \) if and only if it has roots in \( \mathbb{Z}/p^k \mathbb{Z} \). Furthermore, the embedding of \( \mathbb{Z} \) in \( \mathbb{Z}_p \) means that if we can prove that a polynomial has no solutions in \( \mathbb{Z}_p \) for just one \( p \), then there are no solutions in \( \mathbb{Z} \) either, i.e. the existence of a global solution (in \( \mathbb{Z} \)) implies the existence of solutions everywhere locally (i.e. in \( \mathbb{Z}_p \) for every \( p \)). We conclude this chapter with the following theorem.

Theorem 2.2.8 (Hasse-Minkowski). [8, Theorem 3.5.2] Let
\[
f(x_1, \ldots, x_n) \in \mathbb{Q}[x_1, \ldots, x_n]
\]
be a quadratic form (that is, a homogenous polynomial of degree 2 in \( n \) variables). The equation
\[
f(x_1, \ldots, x_n) = 0
\]
has non-trivial solutions in \( \mathbb{Q} \) if and only if it has non-trivial solutions in \( \mathbb{R} \) and \( \mathbb{Q}_p \) for all \( p < \infty \).
Chapter 3

Solving \( ax^3 + by^3 = cz^2 \)

We now present some methods for determining whether an equation of the form \( ax^3 + by^3 = cz^2 \) has primitive solutions. In the case where primitive solutions exist, we demonstrate how to obtain the parametrizing curves that specialise to these solutions. Otherwise, we show how to find an obstruction that is preventing the equation from having primitive solutions. We shall take the coefficients \( a, b, c \) to be square-free integers and note that, without loss of generality, we can assume \( \gcd(a, b, c) = 1 \). Insisting that all of \( a, b, c \) be square-free means that a solution \((x, y, z)\) to \( ax^3 + by^3 = cz^2 \) is primitive if and only if \( x, y \) and \( z \) are pairwise coprime. Let \( h(x, y, z) = ax^3 + by^3 - cz^2 \), we define

\[
D(a, b, c) = \{(x, y, z) \in \mathbb{Z}^3 : h(x, y, z) = 0 \text{ and } \gcd(x, y, z) = 1\}
\]

and

\[
D_p(a, b, c) = \{(x, y, z) \in \mathbb{Z}_p^3 : h(x, y, z) = 0 \text{ and } \min\{\text{ord}_p(x), \text{ord}_p(y), \text{ord}_p(z) = 0\}\}
\]

the sets, respectively, of \( \mathbb{Z} \)-primitive and \( \mathbb{Z}_p \)-primitive solutions of \( ax^3 + by^3 = cz^2 \). We will show in Chapter 4 that \( D_p(a, b, c) \neq \emptyset \) for all \( p \nmid 6abc \) (see Corollary 4.2.6).
CHAPTER 3. SOLVING $AX^3 + BY^3 = CZ^2$

3.1 Local obstructions

Often obstructions to $D(a, b, c)$ being nonempty can be detected locally, that is if we can show that $D_p(a, b, c) = \emptyset$ for some $p$ then we can conclude that there are no primitive solutions to $ax^3 + by^3 = cz^2$. Moreover, when this is the case, we say that there is a local obstruction at $p$.

The most obvious method of obtaining a local obstruction at some prime $p$ is to show that $ax^3 + by^3 = cz^2$ has no solutions modulo $p^k$ with $\min\{\text{ord}_p(x), \text{ord}_p(y), \text{ord}_p(z)\} = 0$, where $k$ is some positive integer. In fact, it is possible to show using Proposition 2.2.4 that there is a $k$ depending on $a, b, c$ such that $D_p(a, b, c) = \emptyset$ if and only if $ax^3 + by^3 = cz^2 \pmod{p^k}$ has no solutions with $\min\{\text{ord}_p(x), \text{ord}_p(y), \text{ord}_p(z)\} = 0$.

Example 1. For every solution to $x^3 + 2y^3 = 13z^2$ modulo 13 we have $x$ and $y$ both congruent to 0, and hence no locally primitive solutions. Thus we have an obstruction at 13 and hence we can conclude that $D(1, 2, 13) = \emptyset$.

As we will see in the subsequent pages, it is possible to have $D = \emptyset$ while $D_p$ is nonempty for all $p$. For these equations having no local obstructions we must turn to other techniques to decide their solvability.

3.2 Class group obstructions

In this section we present a necessary criterion for $D(1, b, c)$ to be nonempty. Analogues exist for $D(a, b, c)$ when $a \neq 1$ but are more complicated to state. The idea for this comes from [6] in which the authors show that for certain choices of $b, c$ and $r$, the equation $x^2 + by^2 = cz^r$ has primitive solutions if and only if this criterion is met. Following their terminology, we say that there exists a class group obstruction if the condition is not met.

Let $[a]$ denote the equivalence class of $a \in J_K$ in $\text{Cl}(K)$ and define $\psi$ to be the canonical map

$$\psi : \text{Cl}(K) \rightarrow \text{Cl}(K)/2\text{Cl}(K)$$

Note that if $[a]$ is in the kernel of $\psi$, then we must have $[a] = 2[b]$ for some $[b]$ in the class group. We can interpret this statement as the class of $a$ being principal modulo squares.
Remark. If the class number of $K$ is odd, then $2\text{Cl}(K) = \text{Cl}(K)$ and hence every class lies in the kernel of $\psi$. In this case obstructions can not arise from the class group of $K$.

For the moment, we restrict ourselves to the case where $c$ is equal to some prime $p$.

Let $K = \mathbb{Q}(\sqrt[3]{-b})$, $\theta = \sqrt[3]{-b}$ and $f = x^3 + b$. We begin by assuming that $(x, y, z)$ is a primitive solution to $x^3 + by^3 = pz^2$. Then note that

$$N_{K/\mathbb{Q}}(x - \theta y) = x^3 + by^3 = pz^2$$

It is straightforward to verify that if $p \nmid (p \cdot \text{disc}(f))$, then $\text{ord}_p(x - \theta y) \equiv 0 \pmod{2}$, see Lemma 3.4.2 for a proof of this. Furthermore, by considering norms, we find that if $p \mid \text{disc}(f)$ then $\text{ord}_p(x - \theta y) = 0$, otherwise we would obtain a contradiction to the primitivity of $x$ and $y$. Lastly, if $3 \nmid \text{disc}(f)$, $p \nmid 3$ and $3\mathcal{O}_K = p^2q$ then it is possible that $pq \mid (x - \theta y)$, however when $3\mathcal{O}_K = p^3$ then it is easy to verify that $\text{ord}_p(x - \theta y) \equiv 0 \pmod{2}$. Therefore we can conclude $\text{ord}_p(x - \theta y) \equiv 0 \pmod{2}$ for all but finitely many $p$.

Suppose $b^2 \not\equiv 1 \pmod{9}$, then the principal ideal $(x - \theta y)$ in $J_K$ must be of the form

$$(x - \theta y) = pZ_1^2$$

where $Z_1$ is some ideal of $\mathcal{O}_K$ and $p$ some ideal lying above $(p)$ for which

$$N_{K/\mathbb{Q}}(p) = p \cdot c^2$$

for some $c \in \mathbb{Z}$. As the degree of the field extension is 3, Proposition 2.1.16 allows us to conclude that the prime decomposition of $p\mathcal{O}_K$ corresponds to one of the following cases

$$p\mathcal{O}_K = \begin{cases} p & \text{inert case} \\ pq & \text{partially split case} \\ p_1p_2p_3 & \text{totally split case} \\ p^2q & \text{partially ramified case} \\ p^3 & \text{totally ramified case} \end{cases}$$

**Proposition 3.2.1.** If $p \neq 3$ and $p\mathcal{O}_K \mid (x - \theta y)\mathcal{O}_K$, then $p \mid x$ and $p \mid y$. 

CHAPTER 3. SOLVING $AX^3 + BY^3 = CZ^2$  

Proof. We first claim that $\mathbb{Z}[\theta] \cap p\mathcal{O}_K = p\mathbb{Z}[\theta]$. By Proposition 2.1.22 this is automatically true for $b^2 \not\equiv 1 \pmod{9}$ and is easily verified for the remaining cases by noting that when $b^2 \equiv 1 \pmod{9}$ the only possible prime appearing in the denominators of the coefficients of $1, \theta, \theta^2$ of an arbitrary element of $\mathcal{O}_K$ is 3. That means there is a well defined morphism

$$\pi : \mathcal{O}_K \longrightarrow \mathbb{F}_p[\theta]$$

with $\ker(\pi) = p\mathcal{O}_K$. Now, since $\mathbb{Z}[\theta] \cap p\mathcal{O}_K = p\mathbb{Z}[\theta]$ and $x - \theta y \equiv 0 \pmod{p}$, it must follow that $p | x$ and $p | y$. □

Remark. As a consequence of the previous proposition, if $p \neq 3$ and $p\mathcal{O}_K | (x - \theta y)\mathcal{O}_K$, then $x$ and $y$ are not coprime and hence $(x, y, z)$ is not primitive at $p$. In particular, when $p$ is inert we have a local obstruction to primitive solutions at $p$.

Example 2. Consider $x^3 + 2y^3 = 7z^2$. Let $\theta = \sqrt[3]{2}$ and $K = \mathbb{Q}(\theta)$. Note that $7\mathcal{O}_K$ is prime, and hence 7 is inert. Using Proposition 3.2.1 we can conclude that for any integer solution $(x, y, z)$ we have $7 | \gcd(x, y)$ and hence the equation has no primitive solutions.

In the partially split case, we have $p\mathcal{O}_K = pq$ and without loss of generality $N(p) = p$ and $N(q) = p^2$. Therefore we have $(x - \theta y) = pZ_1^2$, where $Z_1$ is some ideal of $\mathcal{O}_K$, and hence in $\text{Cl}(\mathcal{O}_K)$ we have

$$[pZ_1^2] = [p] + 2[Z_1]$$

therefore $[p] = -2[Z_1] \in 2\text{Cl}(\mathcal{O}_K)$. Thus we can conclude that $[p] \in \ker(\psi)$. It follows that if $[p]$ is not in the kernel of $\psi$ then the equation has no primitive solutions.

In the totally split case, we have $p\mathcal{O}_K = p_1p_2p_3$ and $N(p_1) = N(p_2) = N(p_3) = p$. Without loss of generality, $(x - \theta y) = p_iZ_1^2$ for one of the $i$’s and hence if no $[p_i]$ lies in the kernel of $\psi$ then we can conclude that the equation has no primitive solutions.

In the partially ramified case, we have $p\mathcal{O}_K = p^2q$, where $N(p) = N(q) = p$. Hence we either have $(x - \theta y) = pZ_1^2$ or $(x - \theta y) = qZ_1^2$. Note that in the class group we have $[qp^2] = [1]$, so that $[q] + 2[p] = [1]$ and therefore $[q] = -2[p]$. Thus $[q]$ clearly lies in the kernel of $\psi$ and so in this case the class group does not preclude primitive solutions to the equation.

In the totally ramified case, we have $p\mathcal{O}_K = p^3$, and $N(p) = p$. Thus we must have
CHAPTER 3. SOLVING $AX^3 + BY^3 = CZ^2$

$(x - \theta y) = pZ_1^2$ or $(x - \theta y)$ and $[p]$ would have to lie in the kernel of $\psi$. But this is always true in this particular case (as $[p^3] = [1] \Rightarrow [p] = -2[p^2]$) and hence this can never lead to a class group obstruction.

We now present some examples of equations having a class group obstruction. In all of the following cases, $D_p(a, b, c) \neq \emptyset$ for all $p$, so that there are no local obstructions. We use the MAGMA computer algebra system [2] to find generators for the prime ideals and to compute their image under $\psi$. We provide the code used to obtain these results in Appendix C.

Example 3. We shall show that $x^3 + 11y^3 = 5z^2$ has no primitive solutions. Let $\theta = \sqrt[3]{11}, K = \mathbb{Q}(\theta)$ and note that $\#\text{Cl}(K) = 2$. Then $5O_K = pq$ where

$$p = (5, 1 + \theta), \quad q = (5, 1 + 4\theta + \theta^2)$$

and neither of these prime ideals is principal. Moreover, $p$ must divide $(x - \theta y)$ and hence its equivalence class in $\text{Cl}(K)$ must lie in the kernel of $\psi$. A simple computation shows that this is not the case and therefore we can conclude that there are no primitive solutions to this equation.

Example 4. We shall show that $x^3 + 113y^3 = 43z^2$ has no primitive solutions. Let $\theta = \sqrt[3]{113}, K = \mathbb{Q}(\theta)$ and note that $\#\text{Cl}(K) = 4$. Then $43O_K = p_1p_2p_3$ where

$$p_1 = (43, 3 + \theta), \quad p_2 = (43, 18 + \theta), \quad p_3 = (43, 22 + \theta)$$

and none of these prime ideals is principal. Now, we know that $(x - \theta y) = p_iZ_1^2$ for one of the $p_i$’s and thus at least one of the $[p_i]$’s must lie in the kernel of $\psi$. However, a simple computation shows that $[p_i] \notin \ker(\psi)$ for each $i$ and thus there are no primitive solutions to this equation.

Note that if $b^2 \equiv 1 \pmod{9}$, so that $3O_K = p^2q$, then the argument we just described still holds, however we must also take into account the possibility that $pq | (x - \theta y)$. We extend this method to more general $c$ as follows. Let $p_1 \ldots p_r$ be a factorisation of $c$ into rational primes. Then there exist prime ideals $p_1, \ldots, p_t$ lying above $p_1, \ldots, p_r$, and possibly 3, such that

$$(x - \theta y) = p_1 \cdots p_tZ_1^2$$
If any of the $p_i$’s are inert in $\mathcal{O}_K$ then, as before, we obtain a local obstruction at those primes. If no $p_i$ is inert, then we consider the combinations of all possible $p_i$’s lying over their respective rational primes, such that the norm equation still holds. If for all possible combinations, $p_1 \cdots p_t \notin \ker(\psi)$, then a class group obstruction has been obtained and we can conclude that $D(a, b, c)$ has no primitive solutions.
3.3 Parametrizing \( ax^3 + by^3 = cz^2 \)

Having seen the classical approach applied to the Pythagorean triples, we now show how the same method applies to equations of signature \((3, 3, 2)\). We begin by solving \( x^3 + y^3 = z^2 \) and note that although this equation was first solved in full by Mordell (See [11, Chapter 25]), the parametrizing curves we present here correspond to those found by Zagier and presented in [1]. Here,

**Theorem 3.3.1 (Zagier).** Let \( x, y, z \) be coprime integers satisfying

\[
x^3 + y^3 = z^2.
\]

Then there exist \( s, t \in \mathbb{Z}[\frac{1}{2}] \) with \((s, t) \not\equiv (0, 0) \pmod{p}\) for any \( p \nmid 6 \) such that one of the following holds:

\[
\begin{cases}
  x \text{ or } y = \frac{1}{4}(s^4 + 6s^2t^2 - 3t^4) \\
  y \text{ or } x = \frac{1}{4}(-s^4 + 6s^2t^2 + 3t^4) \\
  z = \frac{3}{4}st(s^4 + 3t^4) \\
\end{cases}
\]

\[
\begin{cases}
  x \text{ or } y = s^4 + 6s^2t^2 - 3t^4 \\
  y \text{ or } x = -s^4 + 6s^2t^2 + 3t^4 \\
  z = 6st(s^4 + 3t^4) \\
\end{cases}
\]

\[
\begin{cases}
  x \text{ or } y = s(s^3 + 8t^3) \\
  y \text{ or } x = 4t(t^3 - s^3) \\
  \pm z = s^6 - 20s^3t^3 - 8t^6. \\
\end{cases}
\]

**Proof.** We begin by recognizing that if \((x, y, z)\) is a primitive solution to this equation, then we can factor the left hand side to obtain

\[
(x + y)(x^2 - xy + y^2) = z^2
\]
CHAPTER 3. SOLVING $AX^3 + BY^3 = CZ^2$

Now, let $\delta$ be the gcd of $(x + y)$ and $(x^2 - xy + y^2)$. Note that $\delta$ divides both of

$$x^2 + 2y^2 = y(x + y) + (x^2 - xy + y^2)$$
$$y^2 + 2x^2 = x(x + y) + (x^2 - xy + y^2)$$

and therefore also divides

$$3x^2 = 2(y^2 + 2x^2) - (x^2 + 2y^2)$$
$$3y^2 = 2(x^2 + 2y^2) - (y^2 + 2x^2)$$

so that $\delta \mid 3$, as $x$ and $y$ are coprime. Applying the fundamental theorem of arithmetic we have

$$x + y = \delta z_1^2$$
$$x^2 - xy + y^2 = \delta z_2^2$$

where $z_1, z_2$ are coprime integers and $\delta \in \{\pm 1, \pm 3\}$. We can rule out $\delta < 0$ immediately since the expression $x^2 - xy + y^2$ is always positive. Thus we consider the remaining two cases.

**Case 1: $\delta = 3$**

Here we have

$$x^2 - xy + y^2 = 3z_2^2$$

Let $r_1 = \frac{1}{2} + \frac{\sqrt{-3}}{2}$, then we can factor this over $\mathbb{Z}[\frac{1+\sqrt{-3}}{2}]$ as

$$(x - r_1 y)(x - \bar{r}_1 y) = 3z_2^2.$$ 

Moreover, the ring extension that we are working in is a unique factorization domain, so we have

$$x - r_1 y = (\sqrt{-3})(s + t\sqrt{-3})^2$$
where \( s, t \in \mathbb{Z}[\frac{1}{2}] \). Expanding the right hand side and equating coefficients yields

\[
\begin{align*}
x &= -s^2 - 6st + 3t^2 \\
y &= -2(s^2 - 3t^2)
\end{align*}
\]

so that

\[x + y = -3(s + 3t)(s - t).\]

Recall that \( x + y = 3z_1^2 \) and so combining this with the previous statement we obtain

\[z_1^2 = (s + 3t)(t - s).\]

As before, notice that we can write

\[
\begin{align*}
s + 3t &= \epsilon u^2 \\
t - s &= \epsilon v^2
\end{align*}
\]

where \( \epsilon \) is a common divisor of both \( s + 3t \) and \( t - s \) and \( \gcd(u, v) = 1 \). Now, by considering linear combinations of \( s + 3t \) and \( t - s \), it is easy to check that the only possible values for \( \epsilon \) are elements of \( \{ \pm 1, \pm 2, \pm 4 \} \). Furthermore, it is straightforward to verify that negative values of \( \epsilon \) yield the same parametrizations as their corresponding positive values. Therefore it is sufficient to consider the three positive possible values of \( \epsilon \).

If \( \epsilon = 1 \), then \( t = (u^2 + v^2)/4 \) and \( s = (u^2 - 3v^2)/4 \) yielding the following parametrization

\[
\begin{align*}
x &= -\frac{1}{4} \left( u^4 - 6u^2v^2 - 3v^4 \right) \\
y &= \frac{1}{4} \left( u^4 + 6u^2v^2 - 3v^4 \right) \\
z &= \frac{3}{4} (uv) \left( u^4 + 3v^4 \right).
\end{align*}
\]
CHAPTER 3. SOLVING $AX^3 + BY^3 = CZ^2$

If $\epsilon = 2$, then $t = (u^2 + v^2)/2$ and $s = (u^2 - 3v^2)/2$ yielding the following parametrization
\[
\begin{align*}
x &= -(u^4 - 6u^2v^2 - 3v^4) \\
y &= (u^4 + 6u^2v^2 - 3v^4) \\
z &= 6(uv)(u^4 + 3v^4).
\end{align*}
\]

If $\epsilon = 4$, then $t = u^2 + v^2$ and $s = u^2 - 3v^2$ yielding the following parametrization
\[
\begin{align*}
x &= -4(u^4 - 6u^2v^2 - 3v^4) \\
y &= 4(u^4 + 6u^2v^2 - 3v^4) \\
z &= 48(uv)(u^4 + 3v^4).
\end{align*}
\]

As $u, v$ are integers, this parametrization cannot give rise to coprime $x, y, z$, a contradiction.

**Case 2: $\delta = 1$**

In this case we have
\[
x^2 - xy + y^2 = z_2^2
\]
and as before we can write this as
\[
(x - r_1y)(x - \bar{r}_1y) = z_2^2
\]
and so
\[
x - r_1y = (s + \sqrt{-3}t)^2.
\]
Expanding this term and comparing both sides of the equation it is easy to see that
\[
\begin{align*}
x &= s^2 - 2st - 3t^2 \\
y &= -4st.
\end{align*}
\]
Now $x + y = s^2 - 6st - 3t^2$ and recall that $x + y = z_1^2$. Let $r_2 = 3 + 2\sqrt{3}$ and $\mathcal{O} = \mathbb{Z}[r_2]$, then we have
\[
(s - r_2t)(s - \bar{r}_2t) = z_1^2.
\]
It follows that we can write
\[ s - r_2t = \epsilon w^2 \]
\[ s - \bar{r}_2t = \bar{\epsilon}\bar{w}^2 \]
where \( \epsilon \) is square-free. Note, \( N(\epsilon w^2) = N(\epsilon)N(w)^2 = z_1^2 \), so that the norm of \( \epsilon \) must equal a square. Now, suppose \( v \) is an irreducible element of \( \mathcal{O} \) such that \( v \mid \epsilon \), then it is easy to check that we also have \( v \mid \bar{\epsilon} \) since \( v^{2m} \mid| z_1^2 \) for some integer \( m \). Since \( v \) divides both \( \epsilon \) and \( \bar{\epsilon} \), it must also divide any linear combinations of these, hence
\[ v \mid [(s - r_2t) - (s - \bar{r}_2t)] \Rightarrow v \mid (\bar{r}_2 - r_2)t \]
and
\[ v \mid [\bar{r}_2(s - r_2t) - r_2(s - \bar{r}_2t)] \Rightarrow v \mid (\bar{r}_2 - r_2)s. \]
It follows that \( v \mid (\bar{r}_2 - r_2) \), as \( s \) and \( t \) must be coprime, and thus \( v \mid (\epsilon) \). Now, if \( v \) is not a unit in \( \mathcal{O} \), then up to associates \( v = \pm \sqrt{3} \) or \( v = 1 \pm \sqrt{3} \), but for none of these choices is \( N(v) \) equal to a square. It follows that \( \epsilon \) must be a unit in \( \mathcal{O} \). Up to squares, the units of \( \mathcal{O} \) are given by the set \( \{-1, 1, 2 + \sqrt{3}, -2 - \sqrt{3}\} \) and therefore we need to consider each of these possibilities for \( \epsilon \).

If \( \epsilon = -1 \), then writing \( w = u + \sqrt{3}v \) we obtain \( t = uv \) and \( s = -u^2 + 3uv + 3v^2 \) yielding the following parametrization
\[
\begin{align*}
x &= (-v + u)(-3v + u)(3v^2 + u^2) \\
y &= (4uv)(u^2 - 3uv + 3v^2) \\
z &= (u^2 - 3v^2)(9v^4 - 18v^3u^2 + 18v^2u^3 - 6u^3v + u^4).
\end{align*}
\]

For the remaining choices of \( \epsilon \), we obtain the same parametrizations, (with \( x \) and \( y \) interchanged for the cases when \( \epsilon \neq 1 \)). For this final parametrization, taking \( u = t - s \) and \( v = t \), we obtain the third parametrization listed in the statement of the proposition. This completes this exercise of finding a complete list of parameterizations of \( x^3 + y^3 = z^2 \). \( \square \)
3.4 Covering obstructions

In some cases, the equation can have no class group obstructions, solutions existing everywhere locally and yet still fail to have any global solutions. We can show this via something we will call a covering obstruction. We present an example of this phenomenon, but first we establish several results.

**Proposition 3.4.1.** Let $k$ be a field of characteristic 0, let $a, b$ and $c$ be elements of $k$ and let $A = k[\theta] = k[x]/(ax^3 + b)$. Then to any solution of $ax^3 + by^3 = cz^2$, with $x, y, z \in k, xyz \neq 0$, we can associate some $\delta \in A^*/A^{*2}, \lambda \in k^*/k^{*2}$ and parametrizations

$$X_{\delta, \lambda}(s, t), Y_{\delta, \lambda}(s, t), Z_{\delta, \lambda}(s, t)$$

homogeneous of degrees 4, 4 and 6 respectively, such that $x, y, z$ can be obtained from $X_{\delta, \lambda}(s, t), Y_{\delta, \lambda}(s, t), Z_{\delta, \lambda}(s, t)$ by specializing $s, t \in k$. Furthermore, another solution gives rise to the same $\delta, \lambda$ if and only if it can be obtained from the same parametrization.

**Proof.** If $ax^3 + by^3 = cz^2$, then $aN_A/k(x - \theta y) = cz^2$. It follows that

$$x - \theta y = \delta(u_0 + u_1 \theta + u_2 \theta^2)^2$$

for some $u_0, u_1, u_2 \in k, \delta \in A^*$ and clearly any square can absorbed by the $(u_0 + u_1 \theta + u_2 \theta^2)^2$ term, thus the value of $\delta$ is only important up to squares. Letting $u = (u_0, u_1, u_2)$, there exist $Q_i, \delta(u) \in \mathbb{Q}[u_0, u_1, u_2]$ such that

$$\delta(u_0 + u_1 \theta + u_2 \theta^2)^2 = Q_{0, \delta}(u) + Q_{1, \delta}(u) \theta + Q_{2, \delta}(u) \theta^2.$$  

Then we have

$$Q_{0, \delta}(u) = x$$
$$Q_{1, \delta}(u) = -y$$
$$Q_{2, \delta}(u) = 0$$

so that $Q_{2, \delta}$ describes a nonsingular conic in $\mathbb{P}^2$, see Lemma 4.2.2 in Chapter 4. Since our choice of $\delta$ was induced from an actual solution, this conic must have a rational point and
CHAPTER 3. SOLVING $AX^3 + BY^3 = CZ^2$

hence there is a projective parametrization

$$(U_0(s, t) : U_1(s, t) : U_2(s, t))$$

of $Q_{3, 2}$ such that

$$(u_0, u_1, u_2) = (\lambda U_0(s, t), \lambda U_1(s, t), \lambda U_2(s, t))$$

for some $\lambda \in k^*/k^{*2}$. Substituting this back into the $Q_{i, s}'$'s yields the result. The second part of the proposition immediately follows.

Lemma 3.4.2. Let $a, b, c$ be coprime integers, $f(t) = at^3 + b, K = \mathbb{Q}[t]/(f(t))$ and suppose that $ax^3 + by^3 = cz^2$ has a primitive solution $(x, y, z) \in \mathcal{D}(a, b, c)$. If $\mathfrak{p}$ is any prime ideal in $\mathcal{O}_K$ such that $\text{ord}_{\mathfrak{p}}(\text{disc}(f)) = \text{ord}_{\mathfrak{p}}(c) = 0$ and $\theta$ is the image of $t$ in $K$, then $\text{ord}_{\mathfrak{p}}(x - \theta y)$ is even.

Proof. Let $L$ be the splitting field of $f$ and write $\theta_1, \theta_2, \theta_3$ for the roots of $f$ in $L$, we will take $\theta_1 = \theta$. Let $v$ be some prime ideal of $\mathcal{O}_L$ lying over $\mathfrak{p}$. By Proposition 2.1.17, we know that $v$ is unramified, since the polynomial $x^2 + x + 1$ is square-free mod $p$, where $p$ is the rational prime lying below $v$. Furthermore, it is clear that $\mathfrak{p}$ is unramified since it does not divide the discriminant of $f$. We extend the valuation $\text{ord}_{\mathfrak{p}}$ on $K$ to a valuation $\text{ord}_v$ on $L$, and note since the $\mathfrak{p}'$ is unramified, we have $\text{ord}_{\mathfrak{p}}(x - \theta y) = \text{ord}_v(x - \theta y)$. Note that $\min\{\text{ord}_v(x), \text{ord}_v(y)\} = 0$, otherwise $p$ would have to divide both $x$ and $y$ thereby contradicting the primitivity of $(x, y, z)$. Towards a contradiction, suppose that $\text{ord}_v(x - \theta_1 y)$ is odd. Then one of $\text{ord}_v(x - \theta_2 y), \text{ord}_v(x - \theta_3 y)$ must be odd, and the other even, since $\text{ord}_v(ax^3 + by^3) = \text{ord}_v(cz^2) = \text{ord}_v(z^2)$ must be even. Without loss of generality we can assume that $\text{ord}_v(x - \theta_2 y)$ is positive and odd. It follows that

$$\text{ord}_v(x - \theta_2 y - (x - \theta_1 y)) = \text{ord}_v(\theta_1 y - \theta_2 y) = \text{ord}_v(y(\theta_1 - \theta_2)) > 0.$$

This implies that $\text{ord}_v(y(a(\theta_1 - \theta_2)) > 0$ and thus $\text{ord}_{\mathfrak{p}}(y) > 0$, since $a(\theta_1 - \theta_2) \mid a \cdot \text{disc}(f)$. But combining this with our earlier assumption that $\text{ord}_v(x - \theta_1 y) > 0$ we find that $\text{ord}_v(x) > 0$, contradicting our earlier statement that $\min\{\text{ord}_v(x), \text{ord}_v(y)\} = 0$. It follows that $\text{ord}_v(x - \theta y)$ is even, and thus $\text{ord}_{\mathfrak{p}}(x - \theta y)$ is even.

Over the next few pages we take $K = \mathbb{Q}(\theta)$ where $\theta = \sqrt[3]{2}$ and let $\mathcal{O}_K$ denote the ring of integers of $K$. 

Lemma 3.4.3. Suppose that \( x^3 - 2y^3 = 493z^2 \) for some coprime integers \( x, y \) and \( z \). Let \( v \) be any prime in \( \mathcal{O}_K \) with \( \text{ord}_v(\text{disc}(f)) > 0 \). Then \( \text{ord}_v(x - \theta y) = 0 \).

Proof. Note that \( \text{disc}(f) = -2^33^3 \), and suppose that \( v \) is a prime in \( \mathcal{O}_K \) dividing the discriminant of \( f \). Towards a contradiction, suppose that \( \text{ord}_v(x - \theta y) \) is not zero. Then taking the norm of \( x - \theta y \) we find that either 2 or 3 must divide \( z \), depending on \( v \). Reducing the equation modulo 2 and 9 respectively, we find that \( x, y \) and \( z \) are not coprime, a contradiction. Hence \( \text{ord}_v(x - \theta y) = 0 \).

We are now ready to present an example of an equation with a covering obstruction. In this example, \( \mathcal{D}_p(a, b, c) \neq \emptyset \) for all primes \( p \) and there are no obstructions coming from the class group.

Theorem 3.4.4. There are no coprime integers \( x, y \) and \( z \) satisfying

\[
x^3 - 2y^3 = 493z^2.
\]

Proof. Towards a contradiction, suppose that \( \mathcal{D}(1, -2, 493) \neq \emptyset \) and choose any \( (x, y, z) \) in \( \mathcal{D}(1, -2, 394) \). By Proposition 3.4.1 we obtain the following factorization in \( \mathcal{O}_K \):

\[
(x - \theta y)(x^2 + \theta xy + \theta^2 y^2) = 493z^2.
\]

Moreover, we have

\[
x - \theta y = \delta z_1^2
\]

where \( \delta, z_1 \in \mathcal{O}_K \) with \( \delta \) square-free and \( N(\delta) = 493m^2 \) for some \( m \in \mathbb{Z} \). Applying Proposition 3.4.1, we have

\[
Q_{0, \delta}(u) = x
\]
\[
Q_{1, \delta}(u) = -y
\]
\[
Q_{2, \delta}(u) = 0
\]

For each \( \delta \), we use MAGMA to determine whether \( Q_{2, \delta} \) has integral points. If \( Q_{2, \delta} \) has no integer points, then the corresponding \( \delta \) cannot give rise to a parametrization, alternatively if \( Q_{2, \delta}(u) \) does have integral points, MAGMA returns a set of parametrizations for \( u_0, u_1 \) and \( u_2 \), up to some scaling coefficient. This allows us to find \( x = X(s, t) \) and \( y = Y(s, t) \)
respectively and so we check to see if these yield coprime solutions. If we find that the parametrizations for the \( u_i \)’s do not give rise to coprime \( x \) and \( y \) then we conclude that the corresponding \( \delta \) does not give rise to primitive solutions.

Note that by Lemmas 3.4.2 and 3.4.3, we know that \((\delta)\) is not divisible by any prime ideal in \( \mathcal{O}_K \) which doesn’t lie over \( c \). Hence, the only primes dividing \( \delta \) come from the set \( \{\pi_1, \pi_2, \pi'_1, \pi'_2\} \) where

\[
\pi_1 = -1 - \theta + 2\theta^2 \\
\pi'_1 = 1 - 2\theta + 4\theta^2
\]

\[
\pi_2 = -3 + 2\theta + \theta^2 \\
\pi'_2 = 9 - 3\theta + \theta^2
\]

and that these elements have the following norms

\[
N(\pi_1) = 17 \\
N(\pi_2) = 29 \\
N(\pi'_1) = 17^2 \\
N(\pi'_2) = 29^2.
\]

Now, take \( \epsilon = 1 + \theta + \theta^2 \), to be a fundamental unit for \( \mathcal{O}_K \), then \( \{1, -1, \epsilon, -\epsilon\} \) is a complete set of squarefree units of \( \mathcal{O}_K \). Recall that \( N(\delta) = 493m^2 \) and \( \delta \) can be assumed to be square-free, thus it is sufficient to consider the following 8 cases.

Case 1: If \( \delta = \pi_1\pi_2 \), then \( x - \theta y = \pi_1\pi_2z_1^2 \). Expanding the right hand side and comparing coefficients we find that

\[
Q_{2,\delta}(u) = -9u_0^2 + 10u_0u_1 + 9u_1^2 + 18u_0u_2 - 36u_1u_2 + 10u_2^2.
\]

However \( Q_{2,\delta} \) has no solutions modulo 29, and hence no integer solutions. Thus this \( \delta \) gives rise to a covering obstruction.

Case 2: If \( \delta = \pi_1\pi_2\pi'_1 \), then \( x - \theta y = \pi_1\pi_2\pi'_1z_1^2 \). Expanding the right hand side and comparing coefficients we find that

\[
Q_{2,\delta}(u) = 17u_0^2 - 170u_0u_1 + 85u_1^2 + 170u_0u_2 + 68u_1u_2 - 170u_2^2.
\]
Using MAGMA, we obtain the following parametrization for $Q_{2,\delta}$

\[
\begin{align*}
  u_0 &= \lambda(27s^2 + 54st + 25t^2) \\
  u_1 &= \lambda(13s^2 + 20st + 5t^2) \\
  u_2 &= \lambda(8s^2 + 12st + 2t^2).
\end{align*}
\]

Here, $s, t$ are not necessarily integers, however taking $\lambda \in \mathbb{Q}$ we can absorb any denominators into this term and thus assume that $s$ and $t$ are both in $\mathbb{Z}$ and that $\gcd(s, t) = 1$. Substituting these parametrizations for $u_0, u_1, u_2$ into $Q_{0,\delta}$ and $Q_{1,\delta}$ we find

\[
\begin{align*}
  x &= \lambda^2(23375s^4 + 107372s^3t + 186558s^2t^2 + 146404st^3 + 44047t^4) \\
  y &= \lambda^2(-6341s^4 - 42432s^3t - 95574s^2t^2 - 89896st^3 - 30345t^4).
\end{align*}
\]

Let $X = x/\lambda^2, Y = y/\lambda^2$, then note that all coefficients of $X$ and $Y$ are divisible by 17, and moreover that neither of $X/17^2$ and $Y/17^2$ are in $\mathbb{Z}[s, t]$. Thus in order for $x$ and $y$ to be coprime integers, we must introduce a factor of 17 into the denominator of $\lambda$. Now, $\text{ord}_{17}(\lambda^2) = -2$ and thus for $x$ and $y$ to both be integers, there must exist $s$ and $t$ such that $\text{ord}_{17}(X(s, t)), \text{ord}_{17}(Y(s, t)) \geq 2$. However, it is easily verified that $X(s, t)/17 \equiv Y(s, t)/17 \equiv 0 \pmod{17}$ if and only if $s, t$ are both congruent to 0 modulo 17. Furthermore, these choices for $s$ and $t$ can never lead to coprime $x$ and $y$ as these force the valuation of $X$ and $Y$ at 17 to be odd which cannot be compensated for by introducing factors of 17 to the denominator of $\lambda$. It follows that this $\delta$ does not give rise to parametrizations producing coprime $x$ and $y$ and thus does not correspond to any primitive solutions.

Case 3: If $\delta = \pi_1 \pi_2 \pi_2'$, then $x - \theta y = \pi_1 \pi_2 \pi_2' z_1^2$. Expanding the right hand side and comparing coefficients we find that

\[
Q_{2,\delta}(u) = -87u_0^2 + 145u_1^2 + 290u_0u_2 - 348u_1u_2.
\]
CHAPTER 3. SOLVING $AX^3 + BY^3 = CZ^2$

Using MAGMA, we obtain the following parametrization for $Q_{2,\delta}$

\[ u_0 = \lambda(7s^2 + 2st - 5t^2) \]
\[ u_1 = \lambda(3s^2 - 4st - 7t^2) \]
\[ u_2 = \lambda(3s^2 - 5t^2). \]

As before, taking $\lambda \in \mathbb{Q}$ we can assume that $s,t$ are both in $\mathbb{Z}$ and that $\gcd(s,t) = 1$. Substituting these into $Q_{0,\delta}$ and $Q_{1,\delta}$ we find

\[ x = \lambda^2(1885s^4 + 4756s^3t + 5046s^2t^2 + 6612st^3 + 3045t^4) \]
\[ y = \lambda^2(-174s^4 - 4292s^3t - 7656s^2t^2 - 4524st^3 + 174t^4). \]

By the same reasoning as before, we find that for all integers $x$ and $y$ generated by these parametrizations, $\ord_{29}(x), \ord_{29}(y)$ are both greater than 0 and thus $x$ and $y$ are not coprime. It follows that this $\delta$ is locally obstructed at 29.

Case 4: If $\delta = \pi_1\pi_2\pi_1'\pi_2'$, then $x - \theta y = \pi_1\pi_2\pi_1'\pi_2'z_1^2$. Expanding the right hand side and comparing coefficients we find that

\[ Q_{2,\delta}(u) = 493u_0^2 - 1972u_0u_1 + 493u_1^2 + 986u_0u_2 + 1972u_1u_2 - 1972u_2^2. \]

Using MAGMA, we obtain the following parametrization for $Q_{2,\delta}$

\[ u_0 = \lambda(-4s^2 + 2t^2) \]
\[ u_1 = \lambda(-2s^2 + 2st + 2t^2) \]
\[ u_2 = \lambda(-3s^2 + t^2). \]

As before, taking $\lambda \in \mathbb{Q}$ we can assume that $s,t$ are both in $\mathbb{Z}$ and that $\gcd(s,t) = 1$. Substituting these into $Q_{0,\delta}$ and $Q_{1,\delta}$ we find that

\[ x = \lambda^2(-1972s^4 - 11832s^3t - 11832s^2t^2 - 3944st^3) \]
\[ y = \lambda^2(4930s^4 + 7888s^3t + 5916s^2t^2 + 3944st^3 + 986t^4). \]

By the same reasoning as before, we find that for all integers $x$ and $y$ generated by these
parametrizations, \( \text{ord}_{17}(x), \text{ord}_{17}(y) \) are both greater than 0 and thus \( x \) and \( y \) are not coprime. It follows that this \( \delta \) is locally obstructed at 17.

Case 5: If \( \delta = \epsilon \pi_1 \pi_2 \), then \( x - \theta y = \epsilon \pi_1 \pi_2 z_1^2 \). Expanding the right hand side and comparing coefficients we obtain

\[
Q_{2,\delta}(u) = 5u_0^2 - 8u_0u_1 + u_1^2 + 2u_0u_2 + 20u_1u_2 - 8u_2^2
\]

which does not have any solutions modulo 17.

Case 6: If \( \delta = \epsilon \pi_1 \pi_2 \pi'_1 \), then \( x - \theta y = \epsilon \pi_1 \pi_2 \pi'_1 z_1^2 \). Expanding the right hand side and comparing coefficients we find that

\[
Q_{2,\delta}(u) = 17u_0^2 + 68u_0u_1 - 51u_1^2 - 102u_0u_2 + 68u_1u_2 + 68u_2^2.
\]

Using MAGMA, we obtain the following parametrization for \( Q_{2,\delta} \)

\[
\begin{align*}
    u_0 &= \lambda(-10s^2 + 8st) \\
    u_1 &= \lambda(-2s^2 + 2st + 2t^2) \\
    u_2 &= \lambda(-7s^2 + t^2).
\end{align*}
\]

As before, taking \( \lambda \in \mathbb{Q} \) we can assume that \( s, t \) are both in \( \mathbb{Z} \) and that \( \gcd(s, t) = 1 \). Substituting these into \( Q_{0,\delta} \) and \( Q_{1,\delta} \) we find

\[
\begin{align*}
    x &= \lambda^2(6528s^4 + 408s^3t - 2856s^2t^2 + 2312st^3 - 68t^4) \\
    y &= \lambda^2(3162s^4 - 7752s^3t + 1020s^2t^2 - 544st^3 + 306t^4).
\end{align*}
\]

By the same reasoning as before, we find that for all integers \( x \) and \( y \) generated by these parametrizations, \( \text{ord}_{17}(x), \text{ord}_{17}(y) \) are both greater than 0 and thus \( x \) and \( y \) are not coprime. It follows that this \( \delta \) is locally obstructed at 17.

Case 7: If \( \delta = \epsilon \pi_1 \pi_2 \pi'_2 \), then \( x - \theta y = \epsilon \pi_1 \pi_2 \pi'_2 z_1^2 \). Expanding the right hand side and
comparing coefficients we obtain

$$Q_{2, \delta}(u) = 58u_0^2 - 58u_0u_1 - 29u_1^2 - 58u_0u_2 + 232u_1u_2 - 58u_2^2$$

which does not have any solutions modulo 17.

Case 8: If $\delta = \epsilon\pi_1\pi_2\pi_1'\pi_2'$, then $x - \theta y = \epsilon\pi_1\pi_2\pi_1'\pi_2'z_1^2$. Expanding the right hand side and comparing coefficients we obtain

$$Q_{2, \delta}(u) = 986u_0u_1 - 493u_1^2 - 986u_0u_2 + 986u_2^2$$

which has the following parametrization

$$
\begin{align*}
  u_0 &= \lambda(s^2 + st - t^2) \\
  u_1 &= \lambda(s^2 + 2st) \\
  u_2 &= \lambda(s^2 - t^2).
\end{align*}
$$

As before, taking $\lambda \in \mathbb{Q}$ we can assume that $s, t$ are both in $\mathbb{Z}$ and that $\gcd(s, t) = 1$. Substituting these into $Q_0$ and $Q_1$ we find

$$
\begin{align*}
  x &= \lambda^2(493s^4 + 986s^3t + 2465s^2t^2 + 2958st^3 + 1479t^4) \\
  y &= \lambda^2(-493s^4 - 1972s^3t + 1479s^2t^2 + 2958st^3 + 493t^4).
\end{align*}
$$

By the same reasoning as before, we find that for all integers $x$ and $y$ generated by these parametrizations, $\ord_{17}(x), \ord_{17}(y)$ are both greater than 0 and thus $x$ and $y$ are not coprime. It follows that this $\delta$ is locally obstructed at 17.

It follows that no $\delta$ can give rise to primitive solutions and thus we can conclude that $\mathcal{D}(1, -2, 493) = \emptyset.$
Chapter 4

Computational approach

We now describe a computational procedure for determining $\mathcal{D}(a, b, c)$. This approach is derived from the algorithm presented in [3] and so we use the same notation where applicable. We abbreviate $\mathcal{D}(a, b, c)$ to simply $\mathcal{D}$.

4.1 Outline

Let $k$ be a field of characteristic zero, let $f(t) = ax^3 + b$ and $A = k[x]/(f(x))$ and write $\theta$ for the image of $x$ in $A$. We consider the subset of $A^*$ modulo squares with representatives in $A^*$ that have a norm in $\mathbb{Q}$ equal to $c/a$ modulo squares:

$$H_k = \left\{ \delta \in A^*/A^{*2} : N_{A/k}(\delta) = \left(\frac{c}{a}\right) k^{*2} \right\}.$$  

When $k = \mathbb{Q}$, we can define a map $\mathcal{D} \to H_k$. First, we define the partial map

$$\mu : \mathcal{D} \to H_k$$

$$(x, y, z) \mapsto x - \theta y$$

For convenience we write $x - \theta y$ instead of $(x - \theta y)A^{*2}$. Note that this definition does not provide a valid image for any point $(x_1, y_1, 0)$, for any such point we define

$$\mu(x_1, y_1, 0) = (x_1 - \theta y_1) + \tilde{f}(x_1, y_1)$$

where $f(x) = (x - x_1 y_1)\tilde{f}(x)$.  

36
Remark. The set $H_k$ could be empty, as we will soon see this would imply that $D = \emptyset$.

When $k = \mathbb{Q}_p$, we can define a map $D_p \to H_k$. First, we define the partial map

$$\mu_p : D_p \to H_k$$

$$(x, y, z) \mapsto x - \theta y$$

where for convenience we write $x - \theta y$ instead of $(x - \theta y)A^2$. Again, note that this definition does not provide a valid image for any point $(x_1, y_1, 0)$, so for any such point we define

$$\mu_p(x_1, y_1, 0) = (x_1 - \theta y_1) + \tilde{f}(x_1, y_1)$$

where $f(x) = (x - x_1y_1)\tilde{f}(x)$.

Now, taking $k = \mathbb{Q}$ and $K = \mathbb{Q}_p$, the natural map $A \to A \otimes_k K$ induces the commutative diagram

$$\begin{array}{ccc}
D & \xrightarrow{\mu} & H_k \\
\downarrow & & \downarrow \rho_p \\
D_p & \xrightarrow{\mu_p} & H_K
\end{array}$$

We define the Selmer set of $D$

$$\text{Sel}(D) = \{\delta \in H_k : \rho_p(\delta) \in \mu_p(D_p) \text{ for all places } p \text{ of } k\}.$$ 

It is clear then that $\mu(D) \subset \text{Sel}(D)$. In particular, if $\text{Sel}(D)$ is empty then $D$ must also be empty. While this implies that $\text{Sel}(D)$ being nonempty is a necessary condition for $D \neq \emptyset$, we can show that it is also sufficient. We let $S$ be the set of rational primes dividing $6abc$ and $S'$ be the set of prime ideals of $O_k$ lying above $6abc$. Write $H_k(S)$ for the elements $\delta \in H_k$ such that $\text{ord}_p(\rho_p(\delta)) \equiv 0 \pmod{2}$ for all $p \in S$. Lemma 3.4.2 implies that $\text{Sel}(D) \subseteq H_k(S)$ and thus $\text{Sel}(D) \subseteq A(2, S')$. 


Lemma 4.1.1. If $\delta \in \text{Sel}(\mathcal{D})$ and $p \in S$, then there exist $X(s,t), Y(s,t), Z(s,t) \in \mathbb{Z}_p[s,t]$ and $s_p, t_p, \lambda_p \in \mathbb{Z}_p$ such that

$$(x_p, y_p, z_p) = (\lambda_p^2 X(s_p, t_p), \lambda_p^2 Y(s_p, t_p), \lambda_p^3 Z(s_p, t_p))$$

is a locally primitive solution at $p$. Furthermore, there exists a positive integer $k_p$ such that if $s, t \in \mathbb{Z}$ with $s \equiv s_p \pmod{p^{k_p}}$ and $t \equiv t_p \pmod{p^{k_p}}$, then

$$(x, y, z) = (\lambda_p^2 X(s, t), \lambda_p^2 Y(s, t), \lambda_p^3 Z(s, t))$$

is also a locally primitive solution at $p$.

Proof. To begin, we know that since $\delta \in \text{Sel}(\mathcal{D})$, there must exist some $(x_p, y_p, z_p) \in \mathcal{D}_p$ such that $\mu_p(x_p, y_p, z_p) = \rho_p(\delta)$. We will follow the proof of Proposition 3.4.1. We take

$$X = Q_{0,\delta}(u)$$
$$Y = -Q_{1,\delta}(u)$$
$$0 = Q_{2,\delta}(u).$$

Since $\delta$ is unobstructed at all $p$, the conic described by $Q_{2,\delta}(u)$ has a rational point by Hasse-Minkowski. Thus $\{(u_0 : u_1 : u_2) \in \mathbb{P}^2 : Q_{2,\delta} = 0\} \cong \mathbb{P}^1$ and hence we can obtain homogenous quadratic polynomials (in $s$ and $t$) for each coordinate of $u$. From this we obtain $X(s,t), Y(s,t), Z(s,t) \in \mathbb{Z}[s,t]$ of degrees 4, 4 and 6 such that $aX(s,t)^3 + bY(s,t)^3 = cZ(s,t)^2$. Since $\mu(x_p, y_p, z_p) = \rho_p(\delta)$, the second part of Proposition 3.4.1 guarantees that there exist $s_p, t_p, \lambda_p$ such that

$$(x_p, y_p, z_p) = (\lambda_p^2 X(s_p, t_p), \lambda_p^2 Y(s_p, t_p), \lambda_p^3 Z(s_p, t_p))$$

is a locally primitive solution at $p$. By rescaling we can assume that $s_p, t_p \in \mathbb{Z}_p$ and $\min\{\text{ord}_p(s_p), \text{ord}_p(t_p)\} = 0$. Since multiplying $\lambda_p$ by a $p$-adic unit does not affect the primitivity of a solution, we can take $\lambda_p = p^v$ where $\text{ord}_p(\lambda_p) = v$. Next, we show that small $p$-adic perturbations of $s_p, t_p$ do not affect primitivity.
Since \((x_p, y_p, z_p)\) is a locally primitive solution, we have \(\min\{\text{ord}_p(x_p), \text{ord}_p(y_p)\} = 0\). Suppose \(\text{ord}_p(x_p) = 0\) and note that

\[
x_p = \lambda_p^2 X(s_p, t_p) = \lambda_p^2 \sum_{i=0}^{4} a_i s_p^i t_p^{4-i}
\]

where the \(a_i\)'s are the integer coefficients of \(X(s, t)\). Now, let \(k_p\) be any positive integer such that \(k_p > -\text{ord}_p(\lambda_p)\), then we have

\[
\lambda_p^2 X(s_p + s' p^{k_p}, t_p + t' p^{k_p}) = \lambda_p^2 \sum_{i=0}^{4} a_i s_p^i t_p^{4-i} + p^{k_p} \lambda_p^2 \sum a_i q_i
\]

where the \(q_i\)'s are polynomials in \(s_p, t_p, s', t'\) with integer coefficients. It is easily verified that

\[
\text{ord}_p \left( \lambda_p^2 \sum_{i=0}^{4} a_i s_p^i t_p^{4-i} \right) = \text{ord}_p(x_p) = 0
\]

and

\[
\text{ord}_p \left( p^{k_p} \lambda_p^2 \sum a_i q_i \right) = k_p - e + \text{ord}_p \left( \sum a_i q_i \right) > 0
\]

since \(\sum a_i q_i \in \mathbb{Z}_p\). It follows that

\[
\text{ord}_p \left( \lambda_p^2 X(s_p + s' p^{k_p}, t_p + t' p^{k_p}) \right) = 0
\]

and thus if \(s' = s_p + s' p^{k_p}, t' = t_p + t' p^{k_p}\) then

\[
(x'_p, y'_p, z'_p) = \left( \lambda_p^2 X(s'_p, t'_p), \lambda_p^2 Y(s'_p, t'_p), \lambda_p^3 Z(s'_p, t'_p) \right)
\]

is a locally primitive solution at \(p\). The same argument applies when \(\text{ord}_p(y_p) = 0\) and we obtain an analogous result. Thus we can conclude that for any integers \(s, t\) satisfying \(s \equiv s_p \pmod{p^{k_p}}, t \equiv t_p \pmod{p^{k_p}}\), the triple

\[
(x, y, z) = \left( \lambda_p^2 X(s, t), \lambda_p^2 Y(s, t), \lambda_p^3 Z(s, t) \right)
\]

is a locally primitive solution solution at \(p\). \(\square\)
Theorem 4.1.2. If $\text{Sel}(D) \neq \emptyset$ then $D \neq \emptyset$.

Proof. Let $p_1, \ldots, p_r$ denote the primes contained in $S$. By Lemma 4.1.1, for each $p$ there exist $s_p, t_p, \lambda_p, k_p$ corresponding to a locally primitive solution at $p$ and a pair of congruences. Using the Chinese Remainder Theorem, we can find integers $s_0$ and $t_0$ such that

$$s_0 \equiv s_p \pmod{p^{k_p}}$$
$$t_0 \equiv t_p \pmod{p^{k_p}}$$

for every $p_i$. Taking $\lambda = \prod_{i=1}^r p_i^{e_i}$ where $e_i = \text{ord}_{p_i}(\lambda_{p_i})$, we have that

$$(x, y, z) = (\lambda^2 X(s_0, t_0), \lambda^2 Y(s_0, t_0), \lambda^3 Z(s_0, t_0))$$

is a locally primitive solution at every $p_i$. We now show how the existence of $s_0, t_0$ implies the existence of a solution that is locally primitive at every prime.

Suppose that $\gcd(s_0, t_0) \neq 1$ and that $q \notin S$ is some prime dividing both $s_0$ and $t_0$ with $q^r \parallel \gcd(s_0, t_0)$. Now, let $s' = s_0/q^r, t' = t_0/q^r$ and $\lambda' = \lambda q^{2r}$, then

$$(\lambda'^2 X(s', t'), \lambda'^2 Y(s', t'), \lambda'^3 Z(s', t'))$$

so that the triple $(s', t', \lambda')$ gives rise to a solution that is locally primitive at all $p \in S$. Now, it is easily verified that if $(s', t', \lambda')$ gives rise to a locally primitive solution at all $p \in S$, then $(s', t', u\lambda')$ will also give rise to a locally primitive solution at all $p$ provided that $u$ is a unit in $\mathbb{Z}_p$. Taking $u = q^{-2r}$ we see that

$$(\lambda'^2 X(s', t'), \lambda'^2 Y(s', t'), \lambda'^3 Z(s', t'))$$

is a locally primitive solution at all $p \in S$. We can repeat this process for all primes dividing $\gcd(s_0, t_0)$ to obtain that if $s_1 = s_0/\gcd(s_0, t_0), t_1 = t_0/\gcd(s_0, t_0)$, then

$$(\lambda'^2 X(s_1, t_1), \lambda'^2 Y(s_1, t_1), \lambda'^3 Z(s_1, t_1))$$

is a locally primitive solution at all $p \in S$. Hence the congruences that we originally used
to derive $s_0, t_0$ become

$$s \equiv s_{p_i}/ \gcd(s_0, t_0) \pmod{p^{k_{p_i}}}$$
$$t \equiv t_{p_i}/ \gcd(s_0, t_0) \pmod{p^{k_{p_i}}}$$

for each $p_i \in S$. It is clear that $s = s_1$ and $t = t_1$ satisfy all of these congruences and that $\gcd(s_1, t_1) = 1$. All that remains to show is that $s_1$ and $t_1$ give rise to $x$ and $y$ which are locally primitive at all $p \not\in S$.

Take $L = \mathbb{Q}[x]/f((x))$ and let $p$ be some prime not in $S$. Recall that we have

$$x = Q_{0,\delta}(u)$$
$$y = -Q_{1,\delta}(u)$$
$$0 = Q_{2,\delta}(u)$$

where

$$u = [u_0 : u_1 : u_2] = [\lambda U_0(s_1, t_1) : \lambda U_1(s_1, t_1) : \lambda U_2(s_1, t_1)]$$

so that $u$ is a point on the projective conic defined by $Q_{2,\delta}$. We also have $\gcd(s_1, t_1) = 1$, so that $\min\{\operatorname{ord}_p(s_1), \operatorname{ord}_p(t_1)\} = 0$.

Towards a contradiction, suppose that $x \equiv y \equiv 0 \pmod{p}$. Then we have $(x - \theta y) \equiv 0 \pmod{p \mathcal{O}_L}$ and $Q_{0,\delta}(u) \equiv Q_{1,\delta}(u) \equiv Q_{2,\delta} \equiv 0 \pmod{p}$. Now, recall that

$$Q_{0,\delta}(u) + Q_{1,\delta}(u)\theta + Q_{2,\delta}(u)\theta^2 = \delta(u_0 + u_1\theta + u_2\theta^2)^2$$

hence

$$\delta(u_0 + u_1\theta + u_2\theta^2)^2 \equiv 0 \pmod{p \mathcal{O}_L}$$

Now, $\delta$ is a unit in $\mathcal{O}_L/p \mathcal{O}_L$ and since $p \nmid \operatorname{disc}(f)$ we know that $p \mathcal{O}_L$ is unramified, so $\mathcal{O}_L/p \mathcal{O}_L$ has no nilpotent elements and we must have

$$u_0 + u_1\theta + u_2\theta^2 \equiv 0 \pmod{p \mathcal{O}_L}$$
Therefore $u_0 \equiv u_1 \equiv u_2 \equiv 0 \pmod{pO_L}$ and that means that
\[
\begin{align*}
U_0(s_1, t_1) &\equiv 0 \pmod{p} \\
U_1(s_1, t_1) &\equiv 0 \pmod{p} \\
U_2(s_1, t_1) &\equiv 0 \pmod{p}.
\end{align*}
\]

But the $u_i$'s are coordinates on a conic that over $F_p$ is isomorphic to $\mathbb{P}^1$, see Lemma 4.2.2 and Lemma 4.2.3. It follows that $s_1 \equiv t_1 \equiv 0 \pmod{p}$, which is a contradiction since $\gcd(s_1, t_1) = 1$. It follows that $\min\{\text{ord}_p(x), \text{ord}_p(y)\} = 0$ and thus there exists a primitive solution. \hfill \square

### 4.2 Computing $\mu(D_p)$

In this section we assume that $k = \mathbb{Q}_p$ for some prime $p$, that $A = k[x]/(ax^3 + b)$ and we take $S$ to be the set of all primes dividing $6abc$. We will need the following result from algebraic geometry

**Theorem 4.2.1.** [9, Theorem A.4.3.1] Let $C$ be a nonsingular projective conic defined over a field $k$, then $C$ is isomorphic over $k$ to $\mathbb{P}^1$ if and only if it possesses a $k$-rational point.

Let $p$ be some prime not in $S$. As we have already seen, the existence of a primitive solution to $ax^3 + by^3 = cz^2$ gives rise to a factorization $(x - \theta y) = \delta z_1^2$ over the number field $\mathbb{Q}[x]/(ax^3 + b)$, see Proposition 3.4.1. We obtain a corresponding factorization in $\mathbb{Z}_p[\theta]$,

\[
(x - \theta y) = \delta z_1^2
\]

where we take $x, y \in \mathbb{Z}_p$ and $\delta, z_1 \in \mathbb{Z}_p[\theta]$. As before, we write $z_1 = u_0 + u_1 \theta + u_2 \theta^2$ so that

\[
(x - \theta y) = Q_{0,\delta}(u) + Q_{1,\delta}(u)\theta + Q_{2,\delta}(u)\theta^2
\]

with $Q_{2,\delta}$ vanishing for some triple $(u_0, u_1, u_2)$ of elements in $\mathbb{Z}_p$. Now, $Q_{2,\delta}$ is a conic in the projective plane. We claim that $Q_{2,\delta}$ is nonsingular.

**Lemma 4.2.2.** If $p \not\in S$ then $Q_{2,\delta}$ defines a nonsingular conic over $\mathbb{F}_p$ in $\mathbb{P}^2$.

**Proof.** Next we reduce this equation modulo $p$. Let $k = \mathbb{F}_p$ and let $\theta_1, \theta_2, \theta_3$ be the three Galois-conjugates of $\theta$ in the algebraic closure of $k$. Then we have a linear transformation
of vector spaces
\[ T : k[\theta] \rightarrow k[\theta_1] + k[\theta_2] + k[\theta_3] \subset \bar{k} \]
where
\[ T = \begin{pmatrix} 1 & \theta_1 & \theta_1^2 \\ 1 & \theta_2 & \theta_2^2 \\ 1 & \theta_3 & \theta_3^2 \end{pmatrix}. \]

Now, \( x - \theta y = \delta z_1^2 \) for some \( z_1 = u_0 + u_1 \theta + u_2 \theta^2 \in k[\theta] \) if and only if the following equalities hold
\[
x - \theta_1 y = \delta_1 v_1^2 \\
x - \theta_2 y = \delta_2 v_2^2 \\
x - \theta_3 y = \delta_3 v_3^2
\]
where \( v_i = u_0 + u_1 \theta_i + u_2 \theta_i^2 \) and the \( \delta_i \)'s are the images of \( \delta \) under \( T \) for each coordinate.

From this we obtain
\[
(\theta_1 - \theta_3)\delta_2 v_2^2 + (\theta_2 - \theta_1)\delta_3 v_3^2 + (\theta_3 - \theta_2)\delta_1 v_1^2 = 0 \tag{4.1}
\]
and
\[
x = \frac{\theta_2 \delta_1 v_1^2 - \theta_1 \delta_2 v_2^2}{\theta_2 - \theta_1} \quad y = \frac{\delta_1 v_1^2 - \delta_2 v_2^2}{\theta_2 - \theta_1}.
\]

Note that \( T \) is a Vandermonde matrix and hence
\[
\det(T) = \prod_{1 \leq i < j \leq n} (\theta_i - \theta_j)
\]
so that \( T \) is invertible modulo \( p \), since \( p \nmid \text{disc}(f) \). Thus \( T \) defines an isomorphism between the system of equations given by the \( Q_{i,\delta} \)'s in \( \mathbb{F}_p[\theta] \) and the system we have just described. It is easily verified that the projective variety defined by (4.1) is nonsingular if \( \delta_i \neq \delta_j \) and \( \text{ord}_p(\delta) = 0 \), hence \( Q_{2,\delta}(u) = 0 \) also defines a nonsingular conic in \( \mathbb{P}^2 \). □
Lemma 4.2.3. Let \( p \neq 2 \). If \( Q_{2,\delta} \) defines a nonsingular conic over \( \mathbb{F}_p \), then \( Q_{2,\delta} \) has \( p + 1 \) points in \( \mathbb{P}^2 \).

Proof. By completing the square, we obtain an isomorphism between \( Q_{2,\delta} \) and \( C \), where \( C \) is of the form \( U_0^2 = f(U_1, U_2) \) for some homogenous polynomial \( f \in \mathbb{F}_p[U_1, U_2] \). Note that \( C \) must also be nonsingular. If \( C \) has a point, then \( C \) has \( p + 1 \) points, by Proposition 4.2.1, and we are done, so towards a contradiction, assume that \( C \) does not have a point. 

Then for any choice of \( U_1, U_2 \), not both zero, we must have that \( f(U_1, U_2) \) is non-zero and a quadratic non-residue mod \( p \). Let \( C' \subset \mathbb{P}^2 \) defined by \( U_0^2 = m f(U_1, U_2) \) where \( m \in \mathbb{F}_p \) is any quadratic non-residue. Then \( C' \) must have a point as we know that for all choices of \( U_1, U_2 \) we have that \( m f(U_1, U_2) \) is a quadratic residue, and thus \( C' \) has \( p + 1 \) points by Theorem 4.2.1. Now, consider the points \( P \) on \( C' \) of the form \( P = [u_0 : 1 : u_2] \), then there are exactly \( p \) choices for \( U_2 \), as all choices of \( U_1 \) and \( U_2 \) must lead to solutions. Also, note that if \([U_0 : 1 : U_2]\) is a point on \( C' \), then so is \([-U_0 : 1 : U_2]\), and moreover, these points are distinct since \( U_0 \) is never equal to 0. Thus there are at least \( 2p \) distinct points on \( C' \), and thus \( C \) has more than \( p + 1 \) points, a contradiction. It follows that \( C \) always has a point, hence always has \( p + 1 \) points, and thus the projective conic described by \( Q_{\delta,2} \) must also have \( p + 1 \) points. \( \square \)

Lemma 4.2.4. Let \( p \notin S \). If \( Q_{2,\delta} \) defines a nonsingular conic over \( \mathbb{F}_p \) and \( Q_{2,\delta} \) has a nonsingular point \([u_0 : u_1 : u_2] \), then at least one of \( x = Q_{0,\delta}, y = -Q_{1,\delta} \) is nonzero in \( \mathbb{F}_p \).

Proof. Suppose that \( u = [u_0 : u_1 : u_2] \) is a lift to \( \mathbb{Z}_p \) of a projective point on \( Q_{2,\delta} \) mod \( p \). Towards a contradiction, suppose that both \( Q_{0,\delta}(u) \) and \( Q_{1,\delta}(u) \) are divisible by \( p \). Then we have \( x \equiv y \equiv 0 \pmod p \). Let \( k = \overline{\mathbb{F}}_p \), then by Lemma 4.2.2 we have the following

\[
\frac{\theta_2 \delta_1 v_1^2 - \theta_1 \delta_2 v_2^2}{\theta_2 - \theta_1} = \frac{\delta_1 v_1^2 - \delta_2 v_2^2}{\theta_2 - \theta_1} = 0.
\]

Thus

\[
\theta_2 \delta_1 v_1^2 - \theta_1 \delta_2 v_2^2 = \delta_1 v_1^2 - \delta_2 v_2^2 = 0
\]

and hence

\[
\theta_2 \delta_1 v_1^2 - \theta_1 \delta_2 v_2^2 - \theta_2 (\delta_1 v_1^2 - \delta_2 v_2^2) = (\theta_2 - \theta_1) \delta_2 v_2^2 = 0.
\]

Now, since \( p \mid (\theta_2 - \theta_1) \) and \( p \mid \delta_2 \), we must have \( v_2^2 = 0 \) and thus \( v_2 = 0 \), since \( k \) contains no nilpotents. But \( v_2^2 = (u_0 + u_1 \theta_2 + u_2 \theta_2)^2 \), and thus \( v_2 = 0 \) if and only if \( u_0 = u_1 = u_2 = 0 \),
however this does not define a valid projective point \([u_0 : u_1 : u_2]\) in \(\mathbb{P}^2\), a contradiction. \(\square\)

**Theorem 4.2.5.** If \(p \nmid 6abc\) then \(\mu_p(D_p) = \{\delta \in A^*/A^{*2} : \text{ord}_p(\delta) \equiv 0 \pmod{2}\}\).

**Proof.** By the previous lemmas, the reduction of \(Q_{2,\delta}\) has a nonsingular point in \(\mathbb{F}_p\), and therefore must also have a point when considered over \(\mathbb{Z}/p\mathbb{Z}\). Lemma 4.2.4 implies that \(Q_{0,\delta}\) and \(Q_{1,\delta}\) do not simultaneously vanish mod \(p\) for this point. Hensel lifting allows us to obtain a corresponding \((u_0, u_1, u_2) \in \mathbb{Z}_p^3\) such that \(Q_{2,\delta}(u) = 0\), and at least one of \(Q_{0,\delta}(u), Q_{1,\delta}(u)\) nonzero modulo \(p\), and thus we obtain a corresponding point in the local image for this \(\delta\). It follows that the local image contains points corresponding to every \(\delta\), and hence no \(\delta\) can be obstructed at \(p\). Applying Lemma 3.4.2 yields the desired result. \(\square\)

**Corollary 4.2.6.** If \(p \notin S\), then \(D_p(a, b, c) \neq \emptyset\).

For the primes in \(S\) we must do some additional computations to determine the local image. Our approach here relies on the SquareClasses procedure from [3]. Given a square-free \(f(u) \in \mathbb{Z}_p[u]\), let \(A = \mathbb{Q}_p[\theta] = \mathbb{Q}_p[u]/(f(u))\), the SquareClasses procedure returns the image \(\mu(\{(u, v) \in \mathbb{Z}_p^2 : v^2 = f(u)\})\) where \(\mu(u, v) = u - \theta\). This is achieved by building up the possible \(u_1 \in u_0 + p^e\mathbb{Z}_p\) one \(p\)-adic digit at a time. After finitely many steps, Lemma 4.4 in [3] guarantees that the digits that have been fixed for \(u_1\) are sufficient to determine the image \(u_1 - \theta\) in \(A^*/A^{*2}\). We will use the algorithm to find the image of \(d \cdot \mu\) for some \(d \in A^*\). Take \(p\) to be some prime in \(S\). Note that if \(D(a, b, c)\) is non-empty, then so is \(D_p(a, b, c)\). Note that if \((x, y, z) \in D_p\), then \(\min\{\text{ord}_p(x), \text{ord}_p(y)\}\) is equal to zero. Let \(R\) denote the set representatives of \(\mathbb{Z}_p^*/\mathbb{Z}_p^{*2}\) in \(\mathbb{Z}_p^*\), then \(R\) is finite, as per Proposition 2.2.3 and Proposition 2.2.4. We consider the following two cases.

If \(\text{ord}_p(y) = 0\), then we can write \(y = \gamma(D_y)^2\) where \(\gamma, D_y\) are both \(p\)-adic units with \(\gamma \in R\). Then we have

\[
a x^3 + b(\gamma(D_y)^2)^3 = c z^2
\]

and hence dividing all terms by \(D_y^6\) we have

\[
a \left(\frac{x}{D_y^2}\right)^3 + b \gamma^3 = c \left(\frac{z}{D_y^3}\right)^2
\]

and since \(D_y^2\) is a \(p\)-adic unit, \(x/D_y^2\) and \(z/D_y^3\) are both \(p\)-adic integers. Therefore, when \(\text{ord}_p(y) = 0\), we have a correspondence between \((x, y, z) \in D_p\) and primitive local solutions
(\(x', z'\)) to the equation.

\[ aX^3 + b\gamma^3 = cZ^2 \]  \hspace{1cm} (4.2)

where \(x' = x/D_y^2\) and \(z' = z/D_y^3\).

If \(\text{ord}_p(x) = 0\), then we can write \(x = \gamma(D_x)^2\) where \(\gamma \in R\) and \(D_x \in \mathbb{Z}_p\). Therefore, when \(\text{ord}_p(x) = 0\), we have a correspondence between \((x, y, z) \in D_p\) and primitive local solutions \((y', z')\) to the equation.

\[ a\gamma^3 + bY^3 = cZ^2 \]  \hspace{1cm} (4.3)

where \(y' = y/D_x^2\) and \(z' = z/D_x^3\).

For equations (4.1) and (4.2), the SquareClasses procedure allows us to determine the image \((X - \gamma \theta) \in A^*/A^{*2}\) (or \((\gamma - \theta Y) \in A^*/A^{*2}\)). Now when \(\text{ord}_p(y) = 0\) we have

\[(x - \theta y) = (x - \theta \gamma D_y^2) = D_y^2(X - \theta \gamma) = (X - \theta \gamma) \in A^*/A^{*2}\]

and when \(\text{ord}_p(x) = 0\) we have

\[(x - \theta y) = (\gamma D_x^2 - \theta y) = D_x^2(\gamma - \theta Y) = (\gamma - \theta Y) \in A^*/A^{*2}\]

so that in either case we are able to determine the image of \((x - \theta y)\) in \(A^*/A^{*2}\).

We now describe the LocalImage procedure which takes as its input the polynomial \(f(x) = ax^3 + b\).

\textbf{define} LocalImage(f):

1. \(A := \mathbb{Q}_p[\theta] = \mathbb{Q}_p[x]/f(x)\); \(H := A^*/A^{*2}\); \(W := \emptyset\)
2. \(D := \mathbb{Q}_p^*/\mathbb{Q}_p^{*2}\); \(\tilde{\mu} : A^* \to H\)
3. \(R_x := \{x_1 \in \mathbb{Z}_p : ax_1^3 + b = 0\}\)
4. \(\textbf{for} r \in R_x \textbf{ do}\)
5. \(W := W \cup \{\tilde{\mu}(\gamma(r - \theta) + \gamma^2(\frac{c(ax_3 + b)}{x-r})|_{x=\theta}) : \gamma \in D\}\)
CHAPTER 4. COMPUTATIONAL APPROACH

6: end for
7: \( R_y := \{ y_1 \in \mathbb{Z}_p : a + by_1^3 = 0 \} \)
8: for \( r \in R_y \) do
9: \( W := W \cup \{ \tilde{\mu}(\gamma(1-r\theta)) + \gamma^2(\frac{c(a+by)}{1-ry})|_{y=\theta} : \gamma \in D \} \)
10: end for
11: for \( \gamma \in D \) do
12: Set \( \mu_1 : x \mapsto (x - \gamma\theta) \) in \( H \)
13: \( W := W \cup \text{SquareClasses}(c(ax^3 + b\gamma^3), \mu_1) \)
14: Set \( \mu_2 : x \mapsto (\gamma - x\theta) \) in \( H \)
15: \( W := W \cup \text{SquareClasses}(c(a\gamma^3 + bx^3), \mu_2) \)
16: end for
17: return \( W \)

In line 2, \( \tilde{\mu} \) is simply the canonical map from \( A^* \) to \( A^*/A^{*,2} \). In lines 3-10, we determine the image in \( H \) of points of the form \((x_1, y_1, 0)\), considering first those corresponding to \( y \in \mathbb{Z}_p^* \) and second those corresponding to \( x \in \mathbb{Z}_p^* \). In lines 11-16, we use the SquareClasses procedure to determine the local image, following the procedure that we outlined earlier.

### 4.3 Computing \( \text{Sel}(D(k)) \)

In this section, let \( k = \mathbb{Q} \), \( A = \mathbb{Q}[x]/(f(x)) \) and let \( S \) be the set of primes dividing \( 6abc \). We write \( H_k(S) \subset H_k \) for the elements \( \delta \in H_k \) such that \( \text{ord}_v(\rho_v(\delta)) \) is even for all \( v \notin S \). Recall that \( \text{Sel}(D) \subset H_k(S) \). The subgroup \( A(2, S) \subset A^*/A^{*,2} \) of elements with even valuation at all primes outside \( S \) is finite (See [14, VIII] and hence \( H_k(S) \) is also finite. Lemma 3.4.2 guarantees that for any prime \( v \notin S \) we will have \( \rho_v(H_k(S)) \subset \mu_v(D_v) \). Hence

\[
\text{Sel}(D) = \{ \delta \in H_k(S) : \rho_p(\delta) \in \mu_p(D_p) \text{ for all } p \in S \}
\]

This allows us to calculate the Selmer set explicitly.

define ComputeSel(a, b, c):
1: \( A := \mathbb{Q}[x]/(x^3 + \frac{a}{b}) \)
2: Let \( S \) be the set of primes of \( \mathbb{Q} \) described above.
3: \( G := A(2, S) \)
4: \( M := \{ g \in G : N_{A/\mathbb{Q}}(g) \in (c/a)\mathbb{Q}^{*,2} \} \)
5: for $p \in S$ do
6: $A_p := A \otimes \mathbb{Q}_p$, $H_p := A_p^*/A_p^2$
7: $M_p := \text{LocalImage}(f) \subset H_p$
8: Determine $\rho : G \to H_p$
9: $M := \{m \in M : \rho(m) \in M_p\}$
10: end for
11: return $M$

In line 4 we initialize $M$ to include all possible $\delta$. Next, in lines 5-10, we compute the local image $M_p$ at each prime $p \in S$, and eliminate any $\delta \in M$ which does not have a corresponding image in every $M_p$. We return the set $M$ of $\delta$’s which are not obstructed at any prime $p \in S$. By Theorem 4.1.2, these $\delta$’s correspond to parametrizations yielding primitive solutions.

### 4.4 Results

As we have already mentioned, an important application of computing $\text{Sel}(\mathcal{D})$ is that, if it is found to be empty, then we can conclude that $\mathcal{D}$ is also empty and hence that there are no primitive solutions. On the other hand, if the algorithm determines that $\text{Sel}(\mathcal{D})$ is nonempty, Theorem 4.1.2 allows us to conclude that $\mathcal{D}$ is also nonempty. In this section we use $K$ to refer to the number field $\mathbb{Q}(\sqrt[3]{b/a})$. We now present some data and statistics obtained by our implementation of the algorithm in MAGMA. Files for the data presented hereafter, as well as an implementation of our algorithm, can be found at [10].

Note that for many permutations of $a,b,c$ we are solving ‘equivalent’ equations, see Appendix A for a list of equations we deem to be equivalent. This makes it appropriate to impose the following restrictions: $a, b, c$ are all positive, $a \leq b$ and, as usual, $\gcd(a,b,c) = 1$. As we wish to obtain statistics for the occurrence of various obstructions, we insist that $a = 1$ because this simplifies the computation of the class group obstruction. We fix a positive integer $H$ and then determine all $\mathcal{D}(1,b,c)$ where $\max\{b,c\} \leq H$, $\min\{b,c\} \geq 2$, and do this for several $H$ up to 3000, additionally when $\mathcal{D}(a,b,c) = \emptyset$ we determine the obstruction that precludes primitive solutions. First, we present a complete breakdown (see Figure 4.1) for the percentage of $\mathcal{D}(a,b,c)$ nonempty as well as for the various obstructions when $\mathcal{D}(a,b,c)$ is empty. Note that in all all charts presented in this section, values on the
x-axis correspond to values of $H$. For explicit values of the data obtained see Table B.1 in Appendix B.

Figure 4.1: Proportion chart of obstructions, $b, c \leq H$, $H = 20, \ldots, 3000$
Next, from the same set of data, we provide a breakdown (see Figure 4.2) for the obstructions occurring in the cases where the class group in question has even order. The data presented here can be found in Table B.2 in Appendix B. We also provide a breakdown of obstructions for the cases where the class group in question has odd order, see Figure 4.3. The data presented here can be found in Table B.3 in Appendix B. This data suggests that local obstructions are responsible for approximately 85% of total obstructions, with covering and class group obstructions responsible for the remaining 15%. The data also appears to be consistent with respect to the parity of the class group.

Computing $D(a,b,c)$ for all $a,b,c$ bounded above by some given $H$ becomes increasingly slow as we allow $H$ to grow. Therefore, for larger bounds on the coefficients we consider only a random sample of $(a,b,c)$’s rather than an exhaustive set. We bound $H$ by $10^i$ for $i = 4, 5, 6, 7$ and compute 10,000 samples for each $i$. This data is presented in Table 4.1 and Table 4.2 and suggests that equations become increasingly obstructed locally as $H$ increases.
Figure 4.3: Proportion chart of obstructions, \( \#\text{Cl}(K) \) odd, \( b, c \leq H, H = 20, \ldots, 3000 \)

Table 4.1: Random sample data for \( D(a, b, c) \) when \( \#\text{Cl}(K) \) is even

<table>
<thead>
<tr>
<th>( H )</th>
<th>local obs</th>
<th>class group obs</th>
<th>covering obs</th>
<th>total</th>
</tr>
</thead>
<tbody>
<tr>
<td>( 10^4 )</td>
<td>2576</td>
<td>293</td>
<td>137</td>
<td>1257</td>
</tr>
<tr>
<td>( 10^5 )</td>
<td>2924</td>
<td>252</td>
<td>186</td>
<td>1224</td>
</tr>
<tr>
<td>( 10^6 )</td>
<td>3206</td>
<td>238</td>
<td>237</td>
<td>1208</td>
</tr>
<tr>
<td>( 10^7 )</td>
<td>3509</td>
<td>227</td>
<td>225</td>
<td>1112</td>
</tr>
</tbody>
</table>

Table 4.2: Random sample data for \( D(a, b, c) \) when \( \#\text{Cl}(K) \) is odd

<table>
<thead>
<tr>
<th>( H )</th>
<th>local obs</th>
<th>covering obs</th>
<th>total</th>
</tr>
</thead>
<tbody>
<tr>
<td>( 10^4 )</td>
<td>2473</td>
<td>537</td>
<td>2727</td>
</tr>
<tr>
<td>( 10^5 )</td>
<td>2623</td>
<td>489</td>
<td>2302</td>
</tr>
<tr>
<td>( 10^6 )</td>
<td>2533</td>
<td>493</td>
<td>2085</td>
</tr>
<tr>
<td>( 10^7 )</td>
<td>2686</td>
<td>512</td>
<td>1729</td>
</tr>
</tbody>
</table>
Bibliography


52

Appendix A

Equivalent $ax^3 + by^3 = cz^2$

Note that if $ax^3 + by^3 = cz^2$ has primitive solutions, then the following equations must also have primitive solutions

\[
\begin{align*}
ax^3 - by^3 &= cz^2 \\
-ax^3 + by^3 &= cz^2 \\
-ax^3 - by^3 &= cz^2 \\
bx^3 + ay^3 &= cz^2 \\
bx^3 - ay^3 &= cz^2 \\
-bx^3 + ay^3 &= cz^2 \\
-bx^3 - ay^3 &= cz^2 \\
ax^3 + by^3 &= -cz^2 \\
ax^3 - by^3 &= -cz^2 \\
-ax^3 + by^3 &= -cz^2 \\
-ax^3 - by^3 &= -cz^2 \\
bx^3 + ay^3 &= -cz^2 \\
bx^3 - ay^3 &= -cz^2 \\
-bx^3 + ay^3 &= -cz^2 \\
-bx^3 - ay^3 &= -cz^2
\end{align*}
\]
Appendix B

Data tables

In the following tables, $H$ represents a bound for which we determine all $\mathcal{D}(1, b, c)$ where $\max\{b, c\} \leq H$ and $b, c$ both positive, square-free and greater than 1. The figures listed in the other columns represent the number of $\mathcal{D}(1, b, c)$ with $b, c$ bounded by $H$ that meet the specified criteria.

Table B.1: Statistics for $\mathcal{D}(a, b, c)$

<table>
<thead>
<tr>
<th>$H$</th>
<th>Sel($\mathcal{D}$) = $\emptyset$</th>
<th>Sel($\mathcal{D}$) $\neq$ $\emptyset$</th>
<th>total</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>local obs</td>
<td>class group obs</td>
<td>covering obs</td>
</tr>
<tr>
<td>20</td>
<td>37</td>
<td>5</td>
<td>3</td>
</tr>
<tr>
<td>40</td>
<td>181</td>
<td>14</td>
<td>18</td>
</tr>
<tr>
<td>60</td>
<td>359</td>
<td>43</td>
<td>53</td>
</tr>
<tr>
<td>80</td>
<td>823</td>
<td>81</td>
<td>97</td>
</tr>
<tr>
<td>100</td>
<td>1219</td>
<td>130</td>
<td>153</td>
</tr>
<tr>
<td>200</td>
<td>5672</td>
<td>396</td>
<td>623</td>
</tr>
<tr>
<td>300</td>
<td>13074</td>
<td>929</td>
<td>1589</td>
</tr>
<tr>
<td>400</td>
<td>24195</td>
<td>1641</td>
<td>2789</td>
</tr>
<tr>
<td>500</td>
<td>39658</td>
<td>2464</td>
<td>4485</td>
</tr>
<tr>
<td>1000</td>
<td>165363</td>
<td>10118</td>
<td>19478</td>
</tr>
<tr>
<td>1500</td>
<td>386290</td>
<td>22048</td>
<td>45859</td>
</tr>
<tr>
<td>2000</td>
<td>690907</td>
<td>40019</td>
<td>84545</td>
</tr>
<tr>
<td>2500</td>
<td>1106504</td>
<td>60684</td>
<td>133752</td>
</tr>
<tr>
<td>3000</td>
<td>1598049</td>
<td>88062</td>
<td>195347</td>
</tr>
</tbody>
</table>
Table B.2: Statistics for $D(a, b, c)$ when $\#\text{Cl}(K)$ is even

<table>
<thead>
<tr>
<th>$H$</th>
<th>$\text{Sel}(D) = \emptyset$</th>
<th>$\text{Sel}(D) \neq \emptyset$</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>local obs</td>
<td>class group obs</td>
</tr>
<tr>
<td>20</td>
<td>10</td>
<td>5</td>
</tr>
<tr>
<td>40</td>
<td>29</td>
<td>14</td>
</tr>
<tr>
<td>60</td>
<td>93</td>
<td>43</td>
</tr>
<tr>
<td>80</td>
<td>264</td>
<td>81</td>
</tr>
<tr>
<td>100</td>
<td>363</td>
<td>130</td>
</tr>
<tr>
<td>200</td>
<td>2196</td>
<td>396</td>
</tr>
<tr>
<td>300</td>
<td>5151</td>
<td>929</td>
</tr>
<tr>
<td>400</td>
<td>10125</td>
<td>1641</td>
</tr>
<tr>
<td>500</td>
<td>16405</td>
<td>2464</td>
</tr>
<tr>
<td>1000</td>
<td>76612</td>
<td>10118</td>
</tr>
<tr>
<td>1500</td>
<td>181952</td>
<td>22048</td>
</tr>
<tr>
<td>2000</td>
<td>329881</td>
<td>40019</td>
</tr>
<tr>
<td>2500</td>
<td>530852</td>
<td>60684</td>
</tr>
<tr>
<td>3000</td>
<td>783399</td>
<td>88062</td>
</tr>
</tbody>
</table>

Table B.3: Statistics for $D(a, b, c)$ when $\#\text{Cl}(K)$ is odd

<table>
<thead>
<tr>
<th>$H$</th>
<th>$\text{Sel}(D) = \emptyset$</th>
<th>$\text{Sel}(D) \neq \emptyset$</th>
<th>total</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>local obs</td>
<td>covering obs</td>
<td>total</td>
</tr>
<tr>
<td>20</td>
<td>27</td>
<td>3</td>
<td>90</td>
</tr>
<tr>
<td>40</td>
<td>152</td>
<td>18</td>
<td>380</td>
</tr>
<tr>
<td>60</td>
<td>266</td>
<td>52</td>
<td>726</td>
</tr>
<tr>
<td>80</td>
<td>559</td>
<td>89</td>
<td>1165</td>
</tr>
<tr>
<td>100</td>
<td>856</td>
<td>143</td>
<td>1761</td>
</tr>
<tr>
<td>200</td>
<td>3476</td>
<td>552</td>
<td>6378</td>
</tr>
<tr>
<td>300</td>
<td>7923</td>
<td>1375</td>
<td>13816</td>
</tr>
<tr>
<td>400</td>
<td>14070</td>
<td>2379</td>
<td>22997</td>
</tr>
<tr>
<td>500</td>
<td>23253</td>
<td>3802</td>
<td>35775</td>
</tr>
<tr>
<td>1000</td>
<td>88751</td>
<td>15877</td>
<td>127246</td>
</tr>
<tr>
<td>1500</td>
<td>204338</td>
<td>36980</td>
<td>276920</td>
</tr>
<tr>
<td>2000</td>
<td>361026</td>
<td>67390</td>
<td>471158</td>
</tr>
<tr>
<td>2500</td>
<td>575652</td>
<td>105736</td>
<td>724940</td>
</tr>
<tr>
<td>3000</td>
<td>814650</td>
<td>152538</td>
<td>1014413</td>
</tr>
</tbody>
</table>
Appendix C

MAGMA Code

Given square-free integers $b$ and $c$, the following procedure determines whether the equation $x^3 + by^3 = cz^2$ has a class group obstruction.

```magma
function ClObsCheck(b,c)
    LocalObs := false; ClassObs := false;
P<x> := PolynomialRing(Rationals());
K := NumberField(x^3 + b); OK := IntegerRing(K);
Cl,m := ClassGroup(OK);
Cl2,m2 := quo<Cl | 2*Cl>;
ClK := ClassNumber(K);
Candidates := {1*OK};

    if ClK mod 2 eq 0 then
        C := PrimeDivisors(c);

        for i := 1 to #C do
            Fctrs := Factorization(C[i]*OK);

            if #Fctrs eq 1 and Fctrs[1][2] eq 1 then
                return "Equation has a local obstruction";
            end if;
        end for;
    end if;
end function;
```
end if;

// Prime divisors of c which a partially split

if #Fctrs eq 2 then
    Can1 := {}; Can2 := {};
    if Norm(Fctrs[1][1]) eq C[i] and Norm(Fctrs[2][2]) eq 1 then
        I := Fctrs[1][1];
        Can1 := { I*J : J in Candidates};
        end if;
    if Norm(Fctrs[2][1]) eq C[i] and Norm(Fctrs[1][2]) eq 1 then
        I := Fctrs[2][1];
        Can2 := { I*J : J in Candidates};
        end if;
    Candidates := Can1 join Can2;
end if;

// Prime divisors of c which are totally split

if #Fctrs eq 3 then
    I := Fctrs[1][1];
    Can1 := { I*J : J in Candidates};
    I := Fctrs[2][1];
    Can2 := { I*J : J in Candidates};
    I := Fctrs[3][1];
    Can3 := { I*J : J in Candidates};
    Candidates := Can1 join Can2 join Can3;
end if;

end for;

// Include possibility for 3|z^2 when 3 is partially ramified and 3 not dividing c
if $b^2 \mod 9 \equiv 1$ and $c \mod 3 \neq 0$ then

Fctrs := Factorization(3*OK);
I := Fctrs[1][1];
J := Fctrs[2][1];
Can1 := { I*J*L : L in Candidates};
Candidates := Candidates join Can1;
end if;

for SqF in Candidates do
  if SqF@@m in Kernel(m2) then ClassObs := true; end if;
end for;

if ClassObs eq false and LocalObs eq false then
  return "Equation has a class group obstruction";
end if;

return "No Class Group Obstruction";
end if;
end function;

Example:

ClObsCheck(11,5);
Equation has a class group obstruction

Example:

ClObsCheck(113,43);
Equation has a class group obstruction