Université de Montréal

Generalizations of Monsky Matrices for Elliptic Curves in Legendre Form

par

Youcef Mokrani

Département de mathématiques et de statistique
Faculté des arts et des sciences

Mémoire présenté en vue de l'obtention du grade de
Maître ès sciences (M.Sc.)
en mathématiques

Orientation mathématiques fondamentales

April 14, 2020

Université de Montréal

Faculté des arts et des sciences

Ce mémoire intitulé

Generalizations of Monsky Matrices for Elliptic Curves in Legendre Form

présenté par

Youcef Mokrani

a été évalué par un jury composé des personnes suivantes :

Andrew Granville

(président-rapporteur)

Matilde Lalín

(directrice de recherche)

Yvan Saint-Aubin

(membre du jury)

Résumé

Un nombre naturel n est dit congruent si il est l'aire d'un triangle rectangle dont tous les cotés sont de longueur rationnelle. Le problème des nombres congruents consiste à déterminer quels nombres sont congruents. Cette question, connue depuis plus de 1000 ans, est toujours ouverte. Elle est liée à la théorie des courbes elliptiques, car le naturel n est congruent si et seulement si la courbe elliptique $y^2 = x^3 - n^2x$ possède un point rationnel d'ordre infini.

Ce lien entre les nombres congruents et les courbes elliptiques permet d'accéder à des techniques venant de la géométrie algébrique. Une de ces méthodes est le concept des matrices de Monsky qui peuvent être utilisées pour calculer la taille du groupe de 2-Selmer de la courbe elliptique $y^2 = x^3 - n^2x$. On peut utiliser ces matrices afin de trouver de nouvelles familles infinies de nombres non-congruents.

Cette relation introduit aussi des généralisations possibles au problème des nombres congruents. Par exemple, nous pouvons considérer le problème des nombres θ-congruents qui étudie des triangles avec un angle fixé de taille θ au lieu de seulement des triangles rectangles. Ce problème est aussi lié aux courbes elliptiques et le concept des matrices de Monsky peut être étendu à ce cas.

En fait, les matrices de Monsky peuvent être généralisées à n'importe quelle courbe elliptique qui possède une forme de Legendre sur les rationnels. Le but de ce mémoire est de construire une telle généralisation puis de l'appliquer à des problèmes de géométrie arithmétique afin de reprouver efficacement de vieux résultats ainsi que d'en trouver de nouveaux.

Mots clés. Courbes elliptiques, matrices de Monsky, nombres congruents, nombres θ-congruents, 2-descente, groupe de 2-Selmer, théorie des nombres.

Abstract

A positive integer n is said to be congruent if it is the area of a right triangle whose sides are all of rational length. The task of finding which integers are congruent is an old and famous yet still open question in arithmetic geometry called the congruent number problem. It is linked to the theory of elliptic curves as the integer n is congruent if and only if the elliptic curve $y^2 = x^3 - n^2x$ has a rational point of infinite order.

The link between congruent numbers and elliptic curves enables the application of techniques from algebraic geometry to study the problem. One of these methods is the concept of Monsky matrices that can be used to calculate the size of the 2-Selmer group of the elliptic curve $y^2 = x^3 - n^2x$. One can use these matrices in order to find new infinite families of non-congruent numbers.

The connection to elliptic curves also introduces generalizations to the congruent number problem. For example, one may consider the θ-congruent number problem which studies triangles with a fixed angle of θ instead of only right triangles. This problem is also related to elliptic curves and the concept of Monsky matrices can be generalized to it.

In fact, Monsky matrices can be generalized to any elliptic curve that has a Legendre form over the rationals. The goal of this thesis is to construct such a generalization and then to apply it to relevant problems in arithmetic geometry to efficiently reprove old results and find new ones.

Keywords. Elliptic curves, Monsky matrices, congruent numbers, θ-congruent numbers, 2-descent, 2-Selmer group, number theory.

Contents

List of Tables

List of Figures

List of abbreviations

GCD	Greatest common divisor
LI	Linearly independent

Acknowledgments

I am very grateful to Matilde Lalín for her guidance during the last three years. I am especially grateful for the countless corrections she provided for this thesis as it would not exist without them.

I also wish to thank Andrew Granville and Yvan Saint-Aubin for their careful reading and corrections.

I would also like to thank Julien Codsi for some helpful discussions.

Finally, I would like to thank my family for both the material and emotional support that made it possible for me to focus on research.

Introduction

0.1. The main ideas

Let n be a positive integer. We say that n is a congruent number if there exists a right triangle of area n whose sides are all of rational length.

The simplest case of a congruent number is 6, since it is the area of the classic Pythagorean triangle with sides 3, 4 and 5. However, showing that a number is congruent is not always straightforward. For example, 157 is a congruent number, but the simplest triangle that shows this has a hypotenuse of $\frac{2244035177043369699245575130906748631609484720 41}{8912332268928859588025535178967163570016480830}$ [**Zag90**]. Showing that an integer is not congruent is a bit more complicated but can be efficiently done with the use of elliptic curve theory.

A natural question that follows from this definition is to ask which natural numbers are congruent. This question is called the congruent number problem.

The congruent number problem is older than a millennium. Indeed, it was already described in an anonymous Arab manuscript written before 972 (a French translation can be found in [**BWP61**]). However, to this day, the problem remains one of the oldest mathematical questions yet unanswered.

A key property of the congruent number problem that increases its importance is its relation to the theory of elliptic curves. It can be shown that n is congruent if and only if the elliptic curve $y^2 = x^3 - n^2x$ possesses a rational solution with $y \neq 0$ (we will prove this later in Theorem 0.2.2).

Many partial results were found towards the problem, some of which will be presented later in this chapter. The most important of these results is Tunnel's full characterization of the set of congruent numbers [**Tun83**]. It depends on the Birch and Swinnerton-Dyer conjecture which is one of the yet unsolved Millennium Prize Problems.

The congruent number problem can then be seen as a subcase of the Birch and Swinnerton-Dyer conjecture. Because of this, results on the congruent number problem can be used to test the conjecture. Also, potential techniques used to solve the congruent number problem might then be generalized to solve the conjecture.

Several new families of non-congruent numbers were discovered around the end of the 20th century and the start of the 21st. The history of these results is presented in Section 0.2. A method of particular interest for this thesis is the concept of Monsky matrices first presented in [**HB94**]. These matrices were used to find various new families of non-congruent numbers in a very efficient manner.

The relation between the congruent number problem and elliptic curves also leads to generalizations of the problem. One such example is the θ-congruent number problem formulated by Fujiwara [**Fuj02**].

Let $\cos(\theta) = \frac{s}{r}$ such that $r > |s|$ and $GCD(s,r) = 1$. Let n be a positive integer. We say that n is a θ-congruent number if there exists a triangle with an angle of θ whose area is $n\sqrt{r^2 - s^2}$ and whose sides are all of rational length.

Similarly to the case of the congruent number problem, it can be shown that, except for a finite number of small integers, n is θ-congruent if and only if the $y^2 = x(x-n(r-s))(x+n(r+s))$ possesses a rational solution with $y \neq 0$. This relation brings a collection of similar results to those on the congruent number problem. The main result is a full characterization of the set of θ-congruent numbers [**Yos01, Yos02**] when θ is equal to $\frac{\pi}{3}$ or $\frac{2\pi}{3}$. As in the case of the original problem, this result supposes that the Birch and Swinnerton-Dyer conjecture is true.

In [**Mok20**], we showed that the concept of Monsky matrices can also be generalized to the θ-congruent number problem to find new families of non-θ-congruent numbers.

Some of the techniques used in both the congruent number problem and its generalization can be extended to a larger set of elliptic curves. In this thesis, we will be interested in elliptic curves in Legendre form, that have a Weierstrass model of the form $y^2 = (x - e_1)(x - e_2)(x - e_3)$ with $e_1,e_2,e_3 \in \mathbb{Q}$. We will generalize the concept of Monsky matrices to those curves and use the matrices to find new results both on the generalized curves as well as on the congruent number problem. These results are summarized in Chapter 1.

The idea of generalized Monsky matrices can be summarized as follows. Let E be an elliptic curve in Legendre form. Its associated generalized Monsky matrix M is a matrix with elements in $\mathbb{Z}/2\mathbb{Z}$ whose columns and rows depend on the prime factors of the discriminant of E. Generalized Monsky matrices have the property that their kernel has the same size as the 2-Selmer group of their associated elliptic curve. These matrices can then be used to find an upper bound on the rank of elliptic curves in Legendre form. Also, whenever $\dim\ker M = 2$, one can show that the corresponding elliptic curve E is of rank 0.

0.2. The congruent number problem

Since the congruent number problem was already introduced in the preceding section, let us start with a very simple observation on the problem:

Lemma 0.2.1. *Let n and α be positive integers, then n is congruent if and only if $n\alpha^2$ is congruent.*

Proof. If n is congruent then there is a right triangle of rational sides (a,b,c) with area n. We then have that there is a right triangle of sides $(\alpha a, \alpha b, \alpha c)$ of area $n\alpha^2$. This implies that $n\alpha^2$ is also congruent.

We prove the other direction of the statement by dividing the sides by α instead of multiplying. □

Because of the above lemma, we will only be interested in square-free positive integers.

The first major result on the congruent number problem is its relation to an elliptic curve problem. We introduce the concept of elliptic curves in Section 2.3. Here is the result:

Theorem 0.2.2. *A positive integer n is congruent if and only if the elliptic curve*

$$E_n : y^2 = x^3 - n^2 x$$

has a rational point of infinite order, namely, a solution (x,y) with $y \neq 0$.

Proof. An integer n is congruent if and only if the equation system

$$\begin{cases} a^2 + b^2 = c^2, \\ ab = 2n, \end{cases}$$

has a non-trivial rational solution (a,b,$c \in \mathbb{Q}$ and a,b,$c > 0$).

We start by proving the "if" part of the statement. Let there be a right triangle of area n and sides of rational lengths a, b and c. We apply the transformations $X = \frac{n(a+c)}{b}, Y = \frac{2n^2(a+c)}{b^2}$. We then have that

$$\begin{aligned} Y^2 &= \left(\frac{2n^2(a+c)}{b^2}\right)^2 \\ &= \left(\frac{2nX}{b}\right)^2 \\ &= \frac{4n^2X^2}{b^2} \\ &= \frac{(ab)^2X^2}{b^2} \\ &= a^2X^2. \end{aligned}$$

We also have that

$$\begin{aligned} X - \frac{n^2}{X} &= \frac{n(a+c)}{b} - \frac{nb}{(a+c)} \\ &= \frac{n(a+c)^2 - nb^2}{b(a+c)} \\ &= \frac{n(a^2 + c^2 - c^2 + a^2 + 2ac)}{b(a+c)} \\ &= \frac{2n(a^2 + ac)}{b(a+c)} \\ &= \frac{2na}{b} \\ &= a^2. \end{aligned}$$

Combining the two equations gives us that:

$$Y^2 = X^3 - n^2X$$

and this is just E_n.

This means that if n is congruent, then E_n has a rational point with $Y \neq 0$. We can then apply the following proposition:

Proposition 0.2.3 ([**Kob93**] Proven later as Proposition 2.3.9.)**.** *The torsion subgroup of $E_n(\mathbb{Q})$ is of order 4. The subgroup is isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ and its elements are $\mathcal{O}$ (the point at infinity),* $(0{,}0)$*,* $(n{,}0)$ *and* $(-n{,}0)$*.*

Since none of the torsion points have $Y \neq 0$, this implies that if n is congruent, then $Y^2 = X^3 - n^2X$ has a rational solution of infinite order.

We now prove the "only if" part of the statement. If $Y^2 = X^3 - n^2X$ has a rational solution of infinite order $(X{,}Y)$, then $(X'{,}Y') = 2(X{,}Y)$ is also a rational solution of infinite order ($2(X{,}Y)$ being $(X{,}Y) + (X{,}Y)$ with $+$ being the group operation of $E_n(\mathbb{Q})$). The proof of Proposition 2.3.9 then implies that $X' > 0$.

Since $(X'{,}Y')$ is a solution, then $(X'{,} - Y')$ is also a solution. We can then chose the solution $(X{,}Y)$ with $X{,}Y > 0$. Because $Y^2 = X^3 - n^2X$ and $Y{,}X > 0$, we also have that $X^2 > n^2$.

We can then conclude that $a = \frac{X^2 - n^2}{Y}{,}b = \frac{2nX}{Y}{,} c = \frac{(X^2+n^2)}{Y}$ is a solution for the equation system with $a{,}b{,}c \in \mathbb{Q}$ and $a{,}b{,}c > 0$ showing that n is congruent.

□

Because of these results, when we ask if a number n is congruent or not, we will be interested in the associated elliptic curve.

Serf [**Ser91**] applied what is called the method of the 2-descent to the elliptic curve to show that n is congruent if and only if the number of pairs $(b_1{,}b_2) \in \mathbb{Q}(S{,}2) \times \mathbb{Q}(S{,}2)$ for which the equation system

$$\begin{cases} b_1z_1^2 - b_2z_2^2 = n, \\ b_1z_1^2 - b_1b_2z_3^2 = -n, \end{cases}$$

has a non-trivial rational solution is more than four. $\mathbb{Q}(S{,}2)$ can be seen as the set of square-free integers dividing the discriminant of E_n (see Section 2.1 for more details). We show a proof of a generalized version of this result in Section 2.5.

With this knowledge, Serf found sufficient conditions on (b_1,b_2) that guarantee that the above equation system has no solution. Using this, he found infinitely many new non-congruent numbers such as the following family:

Theorem 0.2.4 ([**Ser91**]). *Let p, q and r be distinct primes numbers such that*

$$\begin{cases} p \equiv 1 (\text{mod } 8), \\ q \equiv 3 (\text{mod } 8), \\ r \equiv 3 (\text{mod } 8), \\ \left(\dfrac{p}{q}\right) = -\left(\dfrac{p}{r}\right), \end{cases}$$

then $n = pqr$ is a non-congruent number.

Remark 0.2.5. $\left(\frac{p}{q}\right)$ *is the Legendre Symbol of p by q. See Section 2.7 for more details.*

In 1996, Iskra [**Isk96**] took Serf's methods further and found an infinite family of non-congruent numbers with arbitrarily many prime divisors:

Theorem 0.2.6 ([**Isk96**]). *Let $p_1, \dots, p_\ell$ be distinct primes such that $p_i \equiv 3 \,(\text{mod } 8)$ and $\left(\frac{p_j}{p_i}\right) = -1$ for $j < i$. Then the product $n = p_1 \cdots p_\ell$ is a non-congruent number.*

The proof is a long case by case elimination process that cannot be efficiently replicated to find new families of non-congruent numbers.

Monsky [**HB94**] then developed a matrix whose kernel represents the set of (b_1,b_2) respecting at least one of Serf's conditions of unsolvabilty. We will show how to produce such a matrix in Chapter 4.

It is then possible to show that a number is non-congruent by proving that the corresponding Monsky matrix has a small enough kernel. This is exactly what Reinholz, Spearman and Yang [**RSY13, RSY15, RSY18**] do to find several new families of non-congruent numbers.

0.3. The θ-congruent number problem

Following the preceding section, let us start with a definition from Fujiwara [**Fuj02**]:

Definition 0.3.1. *Let* $\cos(\theta) = \frac{s}{r}$ *such that* $r > |s|$ *and* $GCD(s,r) = 1$*. Let* n *be a positive integer. We say that* n *is a* θ*-congruent number if there exists a triangle with an angle of* θ *whose area is* $n\sqrt{r^2 - s^2}$ *and whose sides are all of rational length.*

This concept is a natural generalization of congruent numbers. We can see that an integer is congruent if and only if it is $\frac{\pi}{2}$-congruent. We can also see the same reduction to square-free integers as before:

Lemma 0.3.2. *Let* n *and* α *be positive integers, then* n *is* θ*-congruent if and only if* $n\alpha^2$ *is* θ*-congruent.*

Proof. If n is θ-congruent the there is a triangle with an angle of θ and sides (a,b,c) with area $n\sqrt{r^2 - s^2}$. We then have that there is a triangle of sides $(\alpha a, \alpha b, \alpha c)$ of area $n\alpha^2$ and the same angles. This implies that $n\alpha^2$ is also θ-congruent.

We prove the other direction of the statement by dividing the sides by α instead of multiplying. □

There are two reasons for which we ask for an area of $n\sqrt{r^2 - s^2}$ instead of simply n.

First, because of the law of cosines, we have to ask that $\cos(\theta)$ is rational in order for all sides to possibly be of rational length. However, if $\sin(\theta)$ is not rational, then the triangle area will trivially be irrational. This is because the area of the triangle is equal to $\frac{ab\sin(\theta)}{2}$ where a and b are the lengths of the sides adjacent to the angle of size θ. In order to avoid this type of trivial contradiction, we multiply the desired area by $r\sin(\theta) = \sqrt{r^2 - s^2}$.

The other reason is that choosing this definition gives us a similar link with elliptic curves:

Theorem 0.3.3. [**Fuj02**] *Let* n *be an integer not dividing 6 and let* θ *be an angle with the same properties as above. Then,* n *is* θ*-congruent if and only if the elliptic curve*

$$y^2 = x(x - n(r - s))(x + n(r + s))$$

has a rational point of infinite order.

The most studied cases of the θ-congruent problem (other than the congruent number problem) are when $\theta = \frac{\pi}{3}$ or $\theta = \frac{2\pi}{3}$. This is because these values of θ are the only rational multiples of π (other than $\frac{\pi}{2}$) for which $\cos(\theta)$ is rational.

From here, we can follow the same steps as in the congruent number problem. We will briefly discuss them here and we will provide more details in Section 2.5.

Indeed, for a fixed angle θ, we can start by applying a 2-descent to have that n is θ-congruent if and only if the number of pairs $(b_1,b_2) \in \mathbb{Q}(S,2) \times \mathbb{Q}(S,2)$ for which the equation system

$$\begin{cases} b_1 z_1^2 - b_2 z_2^2 = n(r-s), \\ b_1 z_1^2 - b_1 b_2 z_3^2 = -n(r+s), \end{cases}$$

has a rational solution is more than four.

Using this fact Girard, Lalín and Nair [**GLN18**] were able to find sufficient conditions on (b_1,b_2) for the above equation system to not have a solution when $\theta = \frac{\pi}{3}$ or $\theta = \frac{2\pi}{3}$. Using such conditions they found the following infinite families of non-θ-congruent numbers:

Theorem 0.3.4 ([**GLN18**])**.** *Let $p_1, \ldots, p_{2\ell+1}$ be distinct primes such that $p_i \equiv 5 \pmod{24}$ and $\left(\frac{p_j}{p_i}\right) = -1$ for $j < i$. Then the product $n = p_1 \cdots p_{2\ell+1}$ is a non-$\frac{\pi}{3}$ congruent number.*

Theorem 0.3.5 ([**GLN18**])**.** *Let $p_1, \ldots, p_{2\ell}$ be distinct primes such that $p_i \equiv 13 \pmod{24}$ and $\left(\frac{p_j}{p_i}\right) = -1$ for $j < i$. Then the product $n = p_1 \cdots p_{2\ell}$ is a non-$\frac{2\pi}{3}$ congruent number.*

However, similarly to Iskra's proof of Theorem 0.2.6, the original proofs of the above theorems are long case by case analyses that are not effectively generalized.

In a previous paper [**Mok20**], we adapted Monsky's matrices to the θ-congruent number problem for $\theta = \frac{\pi}{3}$ and $\theta = \frac{2\pi}{3}$. This made it possible for us to reprove Theorems 0.3.4 and 0.3.5 in an effective manner and it also allowed us to find new families of non-θ-congruent numbers.

0.4. Elliptic curves in Legendre Form

We remark that all the problems we have seen until now are linked to an elliptic curve of the same general form. To be more precise, they are all elliptic curves in Legendre Form.

Definition 0.4.1. *An elliptic curve in Legendre form over the rationals is an elliptic curve written as:*

$$y^2 = (x - e_1)(x - e_2)(x - e_3)$$

with e_1,e_2,$e_3 \in \mathbb{Q}$.

In Chapter 2, we will show that these curves can be reduced to the case $e_1 = 0$ *without changing the structure of the associated group.*

For any given fixed e_1,e_2,e_3, we have a way to do a 2-descent and then create the associated Monsky matrix necessary for our results. However, every time the roots of the elliptic curve change, we have to restart all the work. This is very inefficient.

This takes us to the main goal of this thesis: Develop a general method to construct a matrix whose kernel is in bijection with the 2-Selmer group of any given elliptic curve in Legendre form.

The work to develop such a method is long and arduous. However, once it is done, we will never ever have to do it again as we can then use the same matrices to find new results. Some of these results on the θ-congruent number problem will be also presented in this thesis.

Chapter 1

Main ideas and results

Let us start by explaining the general flow of this thesis.

We will start by introducing some required background for the results of this thesis in Chapter 2. This will be mainly an introduction to elliptic curves with a particular focus on the concept of 2-decent and the 2-Selmer group as well as some other important theorems of number theory such as Hensel's Lemma and Dirichlet's theorem on arithmetic progressions.

Since every elliptic curve with a Legendre form can be reduced to the form $y^2 = x(x-e_2)(x-e_3)$, the method of 2-decent will lead us to the equivalent problem of finding non-trivial rational solutions to the following equation system:

$$\begin{cases} b_1z_1^2 - b_2z_2^2 = e_2, \\ b_1z_1^2 - b_1b_2z_3^2 = e_3. \end{cases}$$

More precisely, we will see that the problem of finding the rank of an elliptic curve is equivalent to finding the number of pairs (b_1,b_2) for which the above system has a solution. In Chapter 3, we will find sufficient conditions on those pairs to guarantee that the equation system has no solution. We will also define a group structure on the (b_1,b_2) respecting all those conditions and show that it is isomorphic to the 2-Selmer group.

Once we have the necessary and sufficient conditions for the above system to have local solutions, we can finally show the main result of this thesis in Chapter 4. This result is the construction of a matrix whose kernel (seen as a group under addition) is isomorphic to the 2-Selmer group of a given elliptic curve in Legendre Form. This construction is done by creating matrix rows representing each of the conditions found in Chapter 3. Since the generation of said matrix takes considerable effort, we will first start by motivating the work by showing some of the interesting results that can be proven using the matrix. The proofs of the results of this section will be presented in Chapter 5.

Since we work often with sizes of 2-Selmer groups, the following definition will be very useful to us:

Definition 1.0.1. *Let e_2 and e_3 be distinct integers. We define $K(e_2,e_3) := \log_2(|Sel_2(E(\mathbb{Q}))|)$, where $Sel_2(E(\mathbb{Q}))$ is the 2-Selmer group of the elliptic curve $E : y^2 = x(x-e_2)(x-e_3)$.*

Most of the time, we will be interested in the cases where $K(e_2,e_3) = 2$ because this implies that there is no rational non-torsion point in the elliptic curve $y^2 = x(x-e_2)(x-e_3)$.

The goal of developing generalized Monsky matrices is to find these cases. For an elliptic curve E in Legendre form, its generalized Monsky matrix M_E is a matrix with terms in $\mathbb{Z}/2\mathbb{Z}$ whose rows and columns depend on the prime factorization of the discriminant of E. This matrix has the important property that the size of its kernel is equal to the size of $\mathrm{Sel}_2(E(\mathbb{Q}))$.

A simple application of the Monsky matrices is finding new families of non-θ-congruent numbers by selecting the prime factors of the discriminant to be in some chosen congruence classes. For example:

Lemma 1.0.2 (Proven later as Lemma 5.3.2)**.** *Let n be a square-free integer that can be factorized as:*

$$n = 6p_1 \cdots p_t q_1 \cdots q_t,$$

where $p_1, \ldots, p_t, q_1, \ldots, q_t$ are distinct primes such that

$$\begin{cases} 2 \nmid t, \\ \forall i, p_i \equiv 7 \pmod{8}, \\ \forall i, q_i \equiv 1 \pmod{8}, \\ \forall i, \left(\dfrac{p_i}{q_i}\right) = -1, \\ \forall i \neq j, \left(\dfrac{p_i}{q_j}\right) = \left(\dfrac{q_i}{q_j}\right) = 1, \\ \forall i, \left(\dfrac{3}{q_i}\right) = -1. \end{cases}$$

Then we have that $K(-2n, -n) = 2$. This implies that n is non-congruent.

The preceding result is new but very similar to some results of Reinholz, Spearman and Yang [**RSY13, RSY15, RSY18**]. We are interested in this particular family of non-congruent numbers because it will be the basis of the proof of Theorem 1.0.5 seen later in this Chapter.

Here is a theorem with more general applications:

Theorem 1.0.3 (Proven later as Theorem 5.1.9)**.** *Let $\mathcal{P}$ be the set of prime numbers. Let e_2, e_3 be two integers such that $GCD(e_2{,}e_3)$ is square-free and $v_2(e_2) > v_2(e_3)$ where $v_2(x)$ indicates the highest exponent of 2 dividing x (this notation will be explained in Section 2.1 and these conditions will be discussed in Section 3.1). Let p,q be distinct prime numbers with the following conditions:*

$$\begin{cases} p{,}q \nmid e_2e_3(e_2 - e_3), \\ p \equiv_8 q, \\ \forall s \mid e_2e_3(e_2 - e_3) \in \mathcal{P}\backslash\{2\}, \left(\dfrac{p}{s}\right) = \left(\dfrac{q}{s}\right). \end{cases}$$

If, additionally, one of the following conditions is respected:

(1) $p \equiv_4 1$ and at least two of $\left\{\left(\frac{e_2}{p}\right), \left(\frac{e_3}{p}\right), \left(\frac{e_3-e_2}{p}\right)\right\}$ are negative.

(2) $p \equiv_4 3$, $\left(\frac{e_3}{p}\right) = -\left(\frac{e_2}{p}\right)$ and $\left(\frac{e_3}{p}\right) = -\left(\frac{e_3-e_2}{p}\right)$.

Then we have that $K(pqe_2{,}pqe_3) = K(e_2{,}e_3)$.

This result is extremely general. It will allow us to find new families of non-θ-congruent number very efficiently. As an example, consider the following corollary:

Corollary 1.0.4. *Let n be an integer that can be factorized in primes as:*

$$n = 2 \cdot 13 \prod_{i=1}^{13} \prod_{j=1}^{\ell_i} p_{i,1,j} p_{i,2,j}$$

with the following conditions:

— $p_{1,k,i} \equiv_8 3$,

— $p_{2,k,i}$, $p_{3,k,i}$, $p_{4,k,i}$, $p_{5,k,i}$, $p_{6,k,i}$ *and* $p_{7,k,i}$ *are congruent to 41, 57, 97, 33, 73 and 89* mod 104 *respectively,*

— $p_{8,k,i}$, $p_{9,k,i}$, $p_{10,k,i}$, $p_{11,k,i}$, $p_{12,k,i}$ *and* $p_{13,k,i}$ *are congruent to 53, 29, 69, 61, 101 and 77* mod 104 *respectively,*

— $(i_1,j_1) \neq (i_2,j_2) \implies \left(\frac{p_{i_1,1,j_1}}{p_{i_2,k,j_2}}\right) = \left(\frac{p_{i_1,2,j_1}}{p_{i_2,k,j_2}}\right)$.

Then n is a non-congruent number.

Also, combining Theorem 1.0.3 and Lemma 1.0.2 gives us the following result:

Theorem 1.0.5 (Proven later as Theorem 5.3.1)**.** *Let n be a square-free integer. There exists a square-free integer m such that $GCD(n,m) = 1$ and nm is non-congruent.*

This result also implies that every integer has an infinite number of non-trivial non-congruent multiples.

Chapter 2

Prerequisites

2.1. Notation

In this section, we define some key notation that will be frequently used in this thesis.

Definition 2.1.1. *We write* $a \equiv_n b$ *to mean* $a \equiv b \pmod{n}$*.*

Definition 2.1.2. *We define* $\mathcal{P}$ *to be the set of all prime numbers.*

Definition 2.1.3. *Let* $n \in \mathbb{Z}$*,* $n \neq 0$ *and* $p \in \mathcal{P}$*. We define the valuation* $v_p(n)$ *to be the largest integer* k *such that* $p^k \mid n$*. We also set that* $v_p(0) = \infty$*.*

Let $x \in \mathbb{Q}$ *that can be written as* $\frac{a}{b}$ *with* $a,b \in \mathbb{Z}$ *and* $b \neq 0$*. We define* $v_p(x) := v_p(a) - v_p(b)$*. Remark that we do not need to take* a *and* b *relatively prime for* v_p *to be well defined.*

The next notation will be very useful in simplifying the text while searching for conditions in prime power moduli.

Definition 2.1.4. *Let* a *be an integer,* k *be a positive integer and* p *be a prime number. When working in* $\mathbb{Z}/p^k\mathbb{Z}$*, we define* $\overline{a}$ *as* $\frac{a}{p^{v_p(a)}}$*. This can be seen as removing the power of* p *dividing* a*.*

Valuations will be very important while discussing p-adic numbers.

Definition 2.1.5. *Let* S *be a finite set of primes. We define:*

$$\mathbb{Q}(S,2) = \{b \in \mathbb{Q}^*/(\mathbb{Q}^*)^2 : \forall p \in \mathcal{P} \backslash S, v_p(b) \equiv_2 0\}$$

where $(\mathbb{Q}^*)^2$ *is the group of non-zero rational numbers with a rational square root under multiplication.*

One can easily see that $\mathbb{Q}(S,2)$ *is a finite abelian group under multiplication.*

2.2. p-adic Numbers

The idea of p-adic numbers provides useful context to this thesis. We will not explicitly need p-adic numbers, but they make some parts of this thesis simpler to explain. They will also bring us to the concept of the local-global principle which we will also discuss in this chapter. For these reasons, we will do a short introduction to p-adic numbers.

Let p be a prime number.

Definition 2.2.1. *We define the set of p-adic integers* $\mathbb{Z}_p$ *as the set of infinite series* $\{a_i\}_{i\in\mathbb{N}}$ *(with* $\mathbb{N}$ *being the set of positive integers) such that:*

$$\begin{cases} a_i \in \mathbb{Z}/p^i\mathbb{Z}, \\ a_i \equiv_{p^i} a_{i+1}. \end{cases}$$

This is a ring with the operations given by component-wise addition and multiplication.

In the literature it is common to summarize the above conditions by saying that $\mathbb{Z}_p$ is the inverse limit of $\mathbb{Z}/p^i\mathbb{Z}$. In other words, $\mathbb{Z}_p := \lim\limits_{\leftarrow i\in\mathbb{N}} \mathbb{Z}/p^i\mathbb{Z}$.

An important fact about p-adic integers is that we can view any integer n as an element of $\mathbb{Z}_p$ by taking the sequence $\{n,n,n,\ldots\}$. We can therefore think of $\mathbb{Z} \subset \mathbb{Z}_p$. This property is the reason we are introducing the concept of p-adic integers and we will return to it later.

Since $\mathbb{Z}_p$ is a domain, we can define the field of fractions of $\mathbb{Z}_p$.

Definition 2.2.2. *The field of p-adic numbers* $\mathbb{Q}_p$ *is the field of fractions of* $\mathbb{Z}_p$*.*

We also consider the limiting case of $p = \infty$ *and define* $\mathbb{Q}_\infty = \mathbb{R}$*.*

Since we have $\mathbb{Z} \subset \mathbb{Z}_p$, we also have the following simple lemma:

Proposition 2.2.3. $\mathbb{Q} \subset \mathbb{Q}_p$

Proof. For $\mathbb{Q}_\infty = \mathbb{R}$ this is trivial by definition.

For the other primes, $\mathbb{Q}$ is the field of fractions of $\mathbb{Z}$ and $\mathbb{Q}_p$ is the field of fractions of $\mathbb{Z}_p$. By the definition of fields of fraction, we have that $\mathbb{Q} \subset \mathbb{Q}_p$ since $\mathbb{Z} \subset \mathbb{Z}_p$. □

The reason this is important to us is the following simple corollary of Proposition 2.2.3:

Corollary 2.2.4. *If an equation system has a solution in $\mathbb{Q}$, then it has a solution in $\mathbb{Q}_p$ for all $p \in \mathcal{P} \cup \{\infty\}$.*

We will return to this corollary when we discuss the local-global principle by the end of this chapter.

2.3. Elliptic Curves

We start by introducing elliptic curves:

Definition 2.3.1. *An elliptic curve over a field K of characteristic 0 is a non-singular curve that can be written as:*

$$y^2 = x^3 + Ax^2 + Bx + C$$

where A,B,$C \in K$.

This definition is not the one typically used. Indeed, it can be shown that all elliptic curves over a field K of characteristic 0 can be written as $y^2 = x^3 + Bx + C$ using a basic variable transformation. However, in this thesis, we will be interested in elliptic curves that have three rational points with $y = 0$. Because of this we will write them as $y^2 = x(x - e_2)(x - e_3)$ to simplify our calculations. For the sake of clarity, we will write elliptic curves as $y^2 = x^3 + Ax^2 + Bx + C$ to avoid the need of transformations further in the thesis.

Since we require a non-singular curve, we add the following result:

Lemma 2.3.2. *A curve $y^2 = x^3 + Ax^2 + Bx + C$ is singular if and only if $\Delta = 16(-4A^3C + A^2B^2 + 18ABC - 4B^3 - 27C^2) = 0$. We call Δ the discriminant of the curve.*

A crucial property of elliptic curves is that the points over the field K form a group denoted by $E(K)$. In this thesis, the two fields that interest us are $\mathbb{R}$, in order to consider graphical representations, and $\mathbb{Q}$. We proceed to describe the group operation.

Definition 2.3.3. *Let $P = (x_1,y_1)$ and $Q = (x_2,y_2)$ be two points on the elliptic curve $y^2 = x^3 + Ax^2 + Bx + C$ with $x_1,x_2,y_1,y_2 \in K$ where K is the given field ($\mathbb{Q}$ or $\mathbb{R}$ in our case). Consider the line passing through P and Q (if $P = Q$, consider the tangent). Let the third point of crossing between the line and the elliptic curve be $R = (x_3,y_3)$. We define $P + Q$ to be $(x_3, -y_3)$.*

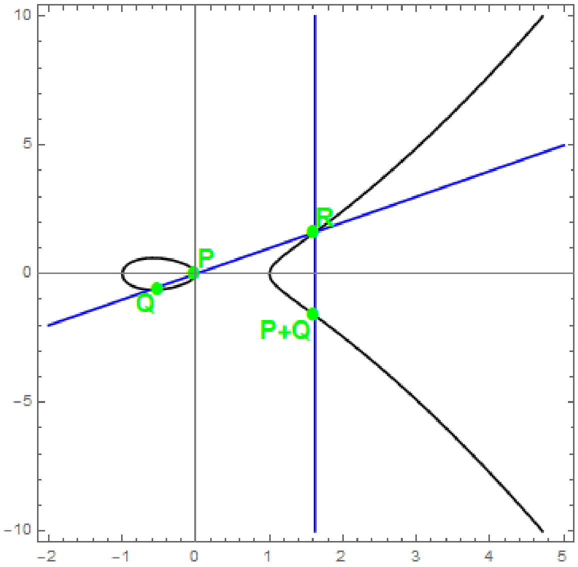

Figure 2.1. An example of the group operation in $E(\mathbb{R})$.

It can be shown that this operation is associative (see [**Sil09**] for a proof). In order for this operation to generate a group, there needs to be a group identity. This can be understood by working in the projective plane $\mathbb{P}_2(K)$ and by representing the affine point (x,y) by the projective point $[x,y,1]$. Every point of $E(K)$ can be represented as a point in $\mathbb{P}_2(K)$. We then define the group identity to be the point at infinity $\mathcal{O} = [0,1,0]$. In the affine space, any line passing by $\mathcal{O}$ and another point P is represented by the vertical line going by P. One can verify that $\mathcal{O}$ defined as such is indeed the group identity (see [**Sil09**] for a proof).

This operation is well defined because, when considering intersection multiplicity, Bézout's theorem (see [**Har77**] for a proof) guarantees the existence of three points of intersection in the projective space between an elliptic curve and a line.

Finally, one can also check that the inverse of the point $P = (x,y)$ is the point $-P = (x, -y)$.

We then have the following result:

Theorem 2.3.4. *Let $E(\mathbb{Q})$ be the set of rational points on the elliptic curve $y^2 = x^3 + Ax^2 + Bx + C$ to which we add $\mathcal{O}$. We then have that $(E(\mathbb{Q}),+)$ is an abelian group.*

Now we consider some transformations that do not change the structure of the group.

Lemma 2.3.5. *Let $E_1 : y^2 = x^3 + Ax^2 + Bx + C$ an elliptic curve and $E_2 : Y^2 = X^3 + AX^2 + BX + C$ where $Y = u^2y$ and $X = u^3x + v$ with $u,v \in \mathbb{Q}$ and $a,c \neq 0$. Then $E_1(\mathbb{Q}) \cong E_2(\mathbb{Q})$.*

We will be interested in the elements of order 2 and 3 in $E(\mathbb{Q})$. The following lemma contains a way to find them.

Lemma 2.3.6. *The points P of order 2 on an elliptic curve are those with $y = 0$.*

The points of order 3 are those with $x(2P) = x(P)$.

Depending on the elliptic curve E, $E(\mathbb{Q})$ does not always have points of order 2 or 3.

We know that $E(\mathbb{Q})$ is always finitely generated. More precisely:

Theorem 2.3.7 (Mordell–Weil [**Wei29**])**.** *We have that:*

$$E(\mathbb{Q}) \cong T \times \mathbb{Z}^r,$$

where r is a non-negative integer called the rank of the elliptic curve and T is a finite group known as the torsion group.

We also have a good understanding of the torsion group:

Theorem 2.3.8 (Mazur [**Maz77, Maz78**])**.** *The torsion subgroup of an elliptic curve defined over $\mathbb{Q}$ is isomorphic to one of the following groups:*

$$\begin{cases} \mathbb{Z}/n\mathbb{Z} \text{ with } 1 \leq n \leq 10, \\ \mathbb{Z}/12\mathbb{Z}, \\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2n\mathbb{Z} \text{ with } 1 \leq n \leq 4. \end{cases}$$

With this result, we can prove Proposition 0.2.3:

Proposition 2.3.9 (Originally Proposition 0.2.3)**.** *Recall that E_n is the elliptic curve $y^2 = x^3 - n^2x$. The torsion subgroup of $E_n(\mathbb{Q})$ is of order 4. The subgroup is isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ and ts elements are $\mathcal{O}$ (the point at infinity),* (0,0)*,* $(n,0)$ *and* $(-n,0)$*.*

Proof. From Corollary 2.3.6, we know that (0,0), $(n,0)$ and $(-n,0)$ are three distinct points of order 2. Mazur's Theorem then implies that the torsion subgroup must be isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2n\mathbb{Z}$ with $1 \leq n \leq 4$. We then only need to show that there is no point of order 3 or 4. We will do this by contradiction.

We start by recalling the formula to calculate $x(2P)$. For the elliptic curve $y^2 = x^3 + Ax^2 + Bx + C$, the duplication formula is:

$$x(2P) = \frac{x^4 - 2Bx^2 - 8Cx + B^2 - 4AC}{4x^3 + 4Ax^2 + 4Bx + 4C}.$$

For the particular family of elliptic curves E_n, the duplication formula is given by

$$x(2P) = \frac{x^4 + 2n^2x^2 + n^4}{4x^3 - 4n^2x} = \left(\frac{x^2 + n^2}{2y}\right)^2.$$

If P were of order 3, we would have that:

$$\begin{aligned} x(P) &= x(2P) \\ x &= \frac{x^4 + 2n^2x^2 + n^4}{4x^3 - 4n^2x} \\ 4x^4 - 4n^2x^2 &= x^4 + 2n^2x^2 + n^4 \\ 3x^4 - 6n^2x^2 - n^4 &= 0 \end{aligned}$$

We can solve this equation for x^2 to obtain that $x^2 = \frac{6n^2 \pm 4n^2\sqrt{3}}{6}$ and, since n is a nonzero integer, we get that there is no rational solution for x and this implies that there is no such rational point P.

If P were of order 4, we would have that $2P \in \{(0,0),(n,0),(-n,0)\}$. This means that $x(2P) \in \{0,n,-n\}$.

We recall that n is a positive integer. Since $x(2P)$ is a strictly positive rational number, $2P \notin \{(0,0),(-n,0)\}$. We then only need the check the equation:

$$\begin{aligned}
x(2P) &= n \\
\frac{x^4+2n^2x^2+n^4}{4x^3-4n^2x} &= n \\
x^4+2n^2x^2+n^4 &= 4nx^3-4n^3x \\
\left(n^2+2nx-x^2\right)^2 &= 0 \\
n^2+2nx-x^2 &= 0 \\
x &= n \pm \sqrt{2}n
\end{aligned}$$

Since $n \in \mathbb{Z}$ and $n \neq 0$, there is no rational solution. This implies that $2P \neq (n,0)$. $2P$ then cannot be of order 2 and this implies that there is no point of order 4.

Since $E_n(\mathbb{Q})$ has no elements of order 3 or 4, we can conclude that its torsion subgroup is $\{\mathcal{O},(0,0),(n,0),(-n,0)\}$. □

2.4. Divisors and Pairings

Section 2.5 contains some statements that are very central for this thesis. We provide here some definitions necessary to understand those results.

The definitions given in this section are only needed for Section 2.5 and will not be used anywhere else, so they will not be given in much detail. One can find more details about them in [**Sil09**] from where they are taken.

We start with the concept of divisors.

Definition 2.4.1. *The divisor group of an elliptic curve $E/\mathbb{Q}$ is the free abelian group generated by the points of E. We denote it by* $\mathrm{div}(E)$. *An element $D \in \mathrm{div}(E)$ can be written as:*

$$\sum_{P \in E(\mathbb{Q})} n_P(P),$$

with $n_P \in \mathbb{Z}$ and $n_P = 0$ for all but finitely many points.

We need the following set of definitions before proceeding to the concept of order.

Definition 2.4.2. *We denote by $\overline{\mathbb{Q}}$ the algebraic closure of $\mathbb{Q}$.*

Definition 2.4.3. *Let $E : y^2 = x^3 + Ax^2 + Bx + C$ be an elliptic curve with coefficients in $\mathbb{Q}$ and let $\overline{\mathbb{Q}}[x,y]$ be the ring of polynomials with coefficients in $\overline{\mathbb{Q}}$*

and two variables. We define the affine coordinate ring of $E/\mathbb{Q}$ to be $\overline{\mathbb{Q}}[E] := \overline{\mathbb{Q}}[x,y]/\left(y^2 - x^3 - Ax^2 - Bx - C\right)$.

The function field $\overline{\mathbb{Q}}(E)$ is the field of fractions of $\overline{\mathbb{Q}}[E]$.

Definition 2.4.4. *For E an elliptic curve, we define the local ring at P to be*

$$\overline{\mathbb{Q}}[E]_P := \left\{ F \in \overline{\mathbb{Q}}(E) : \exists f,g \in \overline{\mathbb{Q}}\,[E] : F = \frac{f}{g} \text{ and } g(P) \neq 0 \right\}.$$

Definition 2.4.5. *M_P is an ideal of $\overline{\mathbb{Q}}[E]$ defined by*

$$M_P := \{f \in \overline{\mathbb{Q}}[E] : f(P) = 0\}.$$

Let d be a positive integer. M_P^d is the subring of $\overline{\mathbb{Q}}[E]$ defined by

$$M_P^d := \{f \in \overline{\mathbb{Q}}[E] : \exists g \in M_P, f = g^d\}.$$

Definition 2.4.6. *Let E be an elliptic curve and $P \in E(\mathbb{Q})$. For $f \in \overline{\mathbb{Q}}[E]_P$, we define $\operatorname{ord}_P(f) = \sup\{d \in \mathbb{Z} : f \in M_P^d\}$.*

For $F \in \overline{\mathbb{Q}}(E)$, we write $F = \frac{f}{g}$ with $f,g \in \overline{\mathbb{Q}}[E]_P$ and we define $\operatorname{ord}_P(F) = \operatorname{ord}_P(f) - \operatorname{ord}_P(g)$.

Definition 2.4.7. *Let E be an elliptic curve and let $f \in \overline{\mathbb{Q}}(E)$. We define the divisor of f as:*

$$\operatorname{div}(f) := \sum_{P \in E(\mathbb{Q})} \operatorname{ord}_P(f)(P).$$

Lemma 2.4.8. *Let E be the elliptic curve $y^2 = (x - e_1)(x - e_2)(x - e_3)$ over $\mathbb{Q}$ and let $f = x - e_i$ with $i \in \{1,2,3\}$, then $\operatorname{div}(f) = 2((e_1,0)) - 2(\mathcal{O})$.*

The other concept that we need to define is pairings.

Definition 2.4.9. *Let G, H and K be groups. A pairing p is a function*

$$p : G \times H \to K,$$

that satisfies bilinearity:

$$\forall g_1,g_2 \in G, \forall h \in H,\ p(g_1g_2,h) = p(g_1,h)p(g_2,h)$$

and

$$\forall g \in G, \forall h_1,h_2 \in H,\ p(g,h_1h_2) = p(g,h_1)p(g,h_2).$$

We say that p is nondegenerate on the left if

$$\forall h \in H, p(g,h) = 1_K \implies g = 1_G.$$

2.5. 2-Descent

From now on, we will only be interested in elliptic curves that can be written in Legendre Form (recall Definition 0.4.1).

Throughout this thesis, we will apply the transformation $x \to x + e_1$ in order to have

$$y^2 = x(x - e_2)(x - e_3).$$

When we use this form, the discriminant is given by $\Delta = 16e_2^2e_3^2(e_3 - e_2)^2$.

Since we have three points of order 2 ((0,0), $(e_2,0)$ and $(e_3,0)$), the torsion subgroup must be of the form $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2m\mathbb{Z}$. This means that $E(\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2m\mathbb{Z} \times \mathbb{Z}^r$. Our goal is to find r.

We will eliminate the m in the torsion point by considering the quotient by the subgroup $2E(\mathbb{Q}) = \{2P : P \in E(\mathbb{Q})\}$.

Theorem 2.5.1. *Let $E(\mathbb{Q})$ be an elliptic curve in Legendre form. We have that:*

$$E(\mathbb{Q})/2E(\mathbb{Q}) \cong (\mathbb{Z}/2\mathbb{Z})^{r+2}.$$

Proof. We know that $E(\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2m\mathbb{Z} \times \mathbb{Z}^r$. We then have that:

$$\begin{aligned} E(\mathbb{Q})/2E(\mathbb{Q}) &\cong (\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2m\mathbb{Z} \times \mathbb{Z}^r)/(2\mathbb{Z}/2\mathbb{Z} \times 2\mathbb{Z}/2m\mathbb{Z} \times (2\mathbb{Z})^r) \\ &\cong ((\mathbb{Z}/2\mathbb{Z})/(2\mathbb{Z}/2\mathbb{Z})) \times ((\mathbb{Z}/2m\mathbb{Z})/(2\mathbb{Z}/2m\mathbb{Z})) \times (\mathbb{Z}/2\mathbb{Z})^r \\ &\cong (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})^r \\ &= (\mathbb{Z}/2\mathbb{Z})^{r+2}. \end{aligned}$$

□

This means that in order to find the rank of the elliptic curve, it is sufficient to study $E(\mathbb{Q})/2E(\mathbb{Q})$. In order to do this, we need the following theorem adapted from [**Sil09**]:

Theorem 2.5.2 (Special case of Theorem 1.1 of Section X.1 in [**Sil09**])**.** *Let $E(\mathbb{Q})$ be an elliptic curve in Legendre form and let $E[2]$ be the 2-torsion of the group $E(\mathbb{Q})$.*

There is a bilinear pairing

$$b : E(\mathbb{Q})/2E(\mathbb{Q}) \times E[2] \to \mathbb{Q}^*/(\mathbb{Q}^*)^2$$

with the following properties:

(1) The pairing b is nondegenerate on the left.

(2) Let S be the set of primes dividing the discriminant of E. The image of b lies in $\mathbb{Q}(S,2)$ (described in Definition 2.1.5).

(3) The pairing b can be computed as follows. For each $T \in E[2]$, choose a function $f_T \in \mathbb{Q}(E)$ such that $\operatorname{div}(f_T) = 2(T) - 2(\mathcal{O})$ and such that there is function $g_T \in \mathbb{Q}(E)$ satisfying $f_T \circ [2] = g_T^2$ ($[2]$ is the function mapping a point on the elliptic curve to its double under the group operation). Such a function f_T exists.

Then for any point $P \neq T$:

$$b(P,T) \equiv f_T(P) \mod (\mathbb{Q}^*)^2.$$

Silverman's version is more general than what we stated above. First, the theorem works for any number field $\mathbb{K}$ and not just $\mathbb{Q}$. Also, the 2 is replaced by an integer $m > 1$ such that $E[m] \subseteq E(\mathbb{K})$. We only need the simpler case above. The original theorem also gives additional properties for b that we do not need and ignoring this additional information spares us from having to discuss the concept of Weil's pairing.

We need the theorem above in order to prove the following result.

Theorem 2.5.3 ([**Sil09**])**.** *Let $E : y^2 = x(x-e_2)(x-e_3)$ defined over $\mathbb{Q}$ be an elliptic curve with $e_2,e_3 \in \mathbb{Q}$. Let S be the set of all primes dividing the discriminant.*

We then have an injective homomorphism $B : E(\mathbb{Q})/2E(\mathbb{Q}) \to \mathbb{Q}(S,2) \times \mathbb{Q}(S,2)$ defined by:

$$B(P) = B((x,y)) = \begin{cases} (x,x-e_2) \text{ if } x \neq 0,e_2, \\ \left(\dfrac{e_3}{e_2},-e_2\right) \text{ if } x = 0, \\ \left(e_2,\dfrac{e_2-e_3}{e_2}\right) \text{ if } x = e_2, \\ (1,1) \text{ if } P = \mathcal{O}. \end{cases}$$

Also, if $(b_1,b_2) \notin \left\{(1,1), \left(\frac{e_3}{e_2},-e_2\right), \left(e_2,\frac{e_2-e_3}{e_2}\right)\right\}$, then (b_1,b_2) is in the image of B if and only if the equation system

$$\begin{cases} b_1z_1^2 - b_2z_2^2 = e_2, \\ b_1z_1^2 - b_1b_2z_3^2 = e_3, \end{cases} \tag{2.5.1}$$

has a solution with $z_1,z_2,z_3 \in \mathbb{Q}$ and $z_1,z_2 \neq 0$. Given such a solution, its preimage is given by $P = (x,y) = (b_1z_1^2,b_1b_2z_1z_2z_3) \in E(\mathbb{Q})$.

Proof. We recall that

$$E[2] = \{\mathcal{O},T_1 = (e_1 = 0,0),T_2 = (e_2,0),T_3 = (e_3,0)\}.$$

The last part of Theorem 2.5.2 gives us a way to determinate the pairing b once we find f_T and g_T with the given conditions. Once we do that, we can simply pose:

$$B(P) = (b(P,T_1),b(P,T_2)).$$

We know from Theorem 2.5.2 that b is bilinear and this implies that B is a morphism. Also, since b is nondegenerate on the left, we have that B is injective. Indeed the kernel of B are the points P such that $(b(P,T_1),b(P,T_2)) = (1,1)$. Since b is bilinear, we have that $b(P,T_1) = b(P,T_2) = b(P,T_3) = b(P,\mathcal{O}) = 1$ and since b is nondegenerate on the left, the only point with this property is $P = \mathcal{O}$.

We now return to work on f_T and g_T. For $i \in \{1,2,3\}$, we define $f_{T_i} = x - e_i$. We remark that $\mathrm{div}(f_{T_i}) = 2(T_i) - 2(\mathcal{O})$.

One can then calculate that

$$\begin{aligned}
f_{T_1} \circ [2](x,y) &= \frac{x^4 - 2e_2e_3x^2 + e_2^2e_3^2}{4x^3 - 4(e_2+e_3)x^2 + 4e_2e_3x} \\
&= \frac{x^4 - 2e_2e_3x^2 + e_2^2e_3^2}{4x(x-e_2)(x-e_3)} \\
&= \frac{(x^2 - e_2e_3)^2}{4y^2} \\
&= \left(\frac{x^2 - e_2e_3}{2y}\right)^2
\end{aligned}$$

and

$$\begin{aligned}
f_{T_2} \circ [2](x,y) &= \frac{x^4 - 2e_2e_3x^2 + e_2^2e_3^2}{4x^3 - 4(e_2+e_3)x^2 + 4e_2e_3x} - e_2 \\
&= \frac{x^4 - 2e_2e_3x^2 + e_2^2e_3^2 - 4x^3e_2 + 4(e_2+e_3)x^2e_2 - 4e_2^2e_3x}{4x(x-e_2)(x-e_3)} \\
&= \frac{x^4 - 4e_2x^3 + (4e_2^2 + 2e_2e_3)x^2 + -4e_2^2e_3x + e_2^2e_3^2}{4x(x-e_2)(x-e_3)} \\
&= \frac{(x^2 - 2e_2x - 2e_2^2 + 2(e_2+e_3)e_2 - (e_2e_3))^2}{4y^2} \\
&= \left(\frac{x^2 - 2e_2x - 2e_2^2 + 2(e_2+e_3)e_2 - e_2e_3}{2y}\right)^2.
\end{aligned}$$

We get $f(T_3)$ by symmetry:

$$f_{T_3} \circ [2](x,y) = \left(\frac{x^2 - 2e_3x - 2e_3^2 + 2(e_2+e_3)e_3 - e_2e_3}{2y}\right)^2.$$

For $i \in \{1,2,3\}$, we can then choose $g_{T_i} = \frac{x^2 - 2e_ix - 2e_i^2 + 2(e_2+e_3)e_i - e_2e_3}{2y}$ and have that the f_{T_i} respect all the required conditions.

Let $P \in E(\mathbb{Q})\backslash E[2]$. We choose $b_1 = b(P,T_1)$ and $b_2 = b(P,T_2)$. Theorem 2.5.2 then implies that

$$\begin{cases} b_1 \equiv x \mod (\mathbb{Q}^*)^2, \\ b_2 \equiv x - e_2 \mod (\mathbb{Q}^*)^2. \end{cases}$$

This implies that there are $z_1,z_2 \in \mathbb{Q}^*$ such that

$$\begin{cases} y^2 = x(x-e_2)(x-e_3), \\ b_1 z_1^2 = x, \\ b_2 z_2^2 = x - e_2. \end{cases}$$

Since $z_1,z_2 \neq 0$, we can define $z_3 = \frac{y}{b_1 b_2 z_1 z_2}$ to get

$$\begin{cases} b_1 b_2 z_3^2 = x - e_3, \\ b_1 z_1^2 = x, \\ b_2 z_2^2 = x - e_2. \end{cases}$$

We can manipulate these equations in order to eliminate x and get

$$\begin{cases} b_1 z_1^2 - b_2 z_2^2 = e_2, \\ b_1 z_1^2 - b_1 b_2 z_3^2 = e_3. \end{cases}$$

If this equation system has a rational solution with $z_1,z_2 \neq 0$, we have that $(b_1,b_2) = B((x,y)) = B((b_1 z_1^2, b_1 b_2 z_1 z_2 z_3))$.

We can then conclude that (b_1,b_2) has a preimage in $E(\mathbb{Q})\backslash E[2]$ if and only if Equation System 2.5.1 has a rational solution with $z_1,z_2,z_3 \in \mathbb{Q}$ and $z_1,z_2 \neq 0$.

We now need to check what happens when $P \in E[2]$. For this, we only need to use the fact that both the given morphism and the pairing are linear.

We have that

$$B(\mathcal{O}) = (1,1),$$

$$\begin{aligned} B(T_1) &= (b(T_1,T_1), b(T_1,T_2)) \\ &= (b(T_1,T_1+T_2)b(T_1,-T_2), b(T_1,T_2)) \\ &= \left(\frac{b(T_1,T_3)}{b(T_1,T_2)}, b(T_1,T_2)\right) \\ &= \left(\frac{-e_3}{-e_2}, -e_2\right) = \left(\frac{e_3}{e_2}, -e_2\right), \end{aligned}$$

$$\begin{aligned}B(T_2) &= (b(T_2,T_1),b(T_2,T_2)) \\ &= \left(b(T_2,T_1),\frac{b(T_2,T_3)}{b(T_2,T_1)}\right) \\ &= \left(e_2,\frac{e_2-e_3}{e_2}\right),\end{aligned}$$

and

$$\begin{aligned}B(T_3) &= B(T_1+T_2) \\ &= B(T_1)B(T_2) \\ &= (e_3,e_3-e_2).\end{aligned}$$

□

We remark that if $z_1 = 0$, the only way to have a solution to Equation System (2.5.1) is when $(b_1,b_2) = \left(\frac{e_3}{e_2}, -e_2\right)$ which is the image of (0,0). Similarly, if $z_2 = 0$, the only way to have a solution is when $(b_1,b_2) = \left(e_2, \frac{e_2-e_3}{e_2}\right)$ which is the image of $(e_2,0)$. Also, if both z_1 and z_2 are equal to 0, there is no solution. This means that it is redundant to ask that $z_1,z_2 \neq 0$ in Theorem 2.5.3.

Since B is an injection, we have that there is a bijection between the image of B and $E(\mathbb{Q})/2E(\mathbb{Q})$. This implies the following lemma.

Lemma 2.5.4. *Let $E(\mathbb{Q}) : y^2 = x(x-e_2)(x-e_3)$ be an elliptic curve with $e_2,e_3 \in \mathbb{Q}$ and let r be its rank. We have that:*

$$r = \log_2\left(|\{(b_1,b_2) \in \mathbb{Q}(S,2) \times \mathbb{Q}(S,2) : \textit{Equation System (2.5.1) has a solution.}\}|\right) - 2.$$

This technique to reduce the problem to an equation system is called the complete 2-descent. From now on, we will be interested in the Equation System (2.5.1) since the techniques of this thesis depend on it.

2.6. Working with the equation system

We recall that the equation system that interests us is given by

$$\begin{cases} b_1z_1^2 - b_2z_2^2 = e_2, \\ b_1z_1^2 - b_1b_2z_3^2 = e_3. \end{cases}$$

For any rational solution $z_1 = \frac{a_1}{d}$,$z_2 = \frac{a_2}{d}$,$z_3 = \frac{a_3}{d}$, with d the common denominator, we can multiply every equation by d^2 to get an equivalent equation system that demands an integer solution with $d \neq 0$:

$$\begin{cases} b_1a_1^2 - b_2a_2^2 = e_2d^2, \\ b_1a_1^2 - b_1b_2a_3^2 = e_3d^2. \end{cases}$$

Also, for the sake of simplifying the notation later, we write a third equation which is the difference of the first two:

$$\begin{cases} b_1a_1^2 - b_2a_2^2 = e_2d^2, \\ b_1a_1^2 - b_1b_2a_3^2 = e_3d^2, \\ b_2a_2^2 - b_1b_2a_3^2 = (e_3 - e_2)d^2. \end{cases}$$

Finding all the pairs (b_1,b_2) whose corresponding system has a non-trivial solution is a difficult problem that does not have a general formula or a quick algorithm that does not depend on the Birch and Swinnerton-Dyer conjecture. However, we have the following lemma:

Lemma 2.6.1. *A necessary condition for an equation system defined over $\mathbb{Z}$ to have a non trivial integral solution is that it has a non trivial solution in $\mathbb{R}$ as well as in $\mathbb{Z}/n\mathbb{Z}$ for all $n \in \mathbb{N}$.*

Proof. If an equation system has an integer solution, then it has a real solution since $\mathbb{Z} \subset \mathbb{R}$.

If an equation has an integer solution (a_1,a_2,a_3,d), a solution in $\mathbb{Z}/n\mathbb{Z}$ is obtained by reducing a_1, a_2, a_3 and d modulo n. □

Lemma 2.6.1 can be used to prove that the equation system of a pair (b_1,b_2) has no solution. This will imply that the pair has no preimage. We already know the four pairs (b_1,b_2) whose preimage is in the torsion subgroup. If one can show that these four pairs are the only ones with a preimage, one will show that the rank of the elliptic curve is 0. This is the main strategy in this thesis since the matrix that we construct will have the role of counting the number of pairs (b_1,b_2) with non trivial solutions in all local fields. This will be explained in further detail in Chapter 4.

Remark that this is very similar to Corollary 2.2.4 that claims that an equation system having a solution in $\mathbb{Q}$ has a solution in $\mathbb{Q}_p$ for all $p \in \mathcal{P} \cup \{\infty\}$. In fact it would have been possible to directly work with Equation System (2.5.1) and show that there is no solution in $\mathbb{Q}_p$ for some $p \in \mathcal{P} \cup \{\infty\}$. We work with the same idea but we prefer to work with integers in this thesis since it makes finding the conditions on the matrix simpler.

This strategy calls for the following definition:

Definition 2.6.2. *We define the 2-Selmer group of an elliptic curve $E(\mathbb{Q})$ as the group of the pairs (b_1,b_2) for which Equation System (3.1.1) has a solution in all $\mathbb{Q}_p$. We will denote it by $Sel_2(E(\mathbb{Q}))$.*

Since the set of pairs (b_1,b_2) whose equation system has a rational solution is a subgroup of $\mathrm{Sel}_2(E(\mathbb{Q}))$, we know that we have a monomorphism yielding the exact sequence

$$0 \to E(\mathbb{Q})/2E(\mathbb{Q}) \xrightarrow{\psi} \mathrm{Sel}_2(E(\mathbb{Q})).$$

If we call this morphism ψ, we can define the 2-torsion of the Tate-Shafarevich group of E, denoted $\text{Ш}(E(\mathbb{Q}))[2]$, to be the cokernel of ψ. That is, a group such that the following sequence is exact:

$$0 \to E(\mathbb{Q})/2E(\mathbb{Q}) \xrightarrow{\psi} \mathrm{Sel}_2(E(\mathbb{Q})) \to \text{Ш}(E(\mathbb{Q}))[2] \to 0.$$

This is not the classical definition of $\text{Ш}(E(\mathbb{Q}))$ but it is equivalent and considerably simpler to explain. We only use it to give some context and we will not go deeper into it.

Before concluding this section, we want to discuss a natural question that derives from Lemma 2.6.1. Is the reciprocity true? If an equation system has a solution for all $\mathbb{Q}_p$, does it have a rational solution? This is what is known as the local-global principle.

For some equation systems, this principle is true. For example the equation $ax^2 + by^2 = cz^2$ with $a,b,c \in \mathbb{Q}$ has a non-trivial solution in $\mathbb{Q}$ if and only if it has a non-trivial solution for every $\mathbb{Q}_p$ including $\mathbb{Q}_\infty = \mathbb{R}$. This proof is attributed to Legendre [**Leg08**].

However, when it comes to elliptic curves, the principle is false, even if we restrict ourselves to elliptic curves in Legendre form. For example, it is proven in [**LT00**] that the elliptic curve $y^2 = x(x-n)(x+n)$ has rank 0 but a Tate-Shafarevich group with a non-trivial 2-torsion when $n = 17 \times 73 \times 97 = 120377$. Since the 2-torsion of the Tate-Shafarevich group is non-trivial, the above exact sequence implies that there are strictly more elements in $\mathrm{Sel}_2(E(\mathbb{Q}))$ than in $E(\mathbb{Q})/2E(\mathbb{Q})$. This means that there are non-trivial solutions in all $\mathbb{Q}_p$ even if there is no non-trivial solution in $\mathbb{Q}$.

This means that the methods developed in this thesis can guarantee that some elliptic curves have no infinite order rational points, but they can never guarantee that an elliptic curve has infinite order rational points.

2.7. Quadratic residues

A question that will be asked often in this thesis is whether a number is a square in $\mathbb{Z}/p\mathbb{Z}$ with p a given prime. To simplify the text, consider the following definition:

Definition 2.7.1. *We say that an integer a is a quadratic residue in $\mathbb{Z}/p\mathbb{Z}$ if there exists an integer k such that $k^2 \equiv_p a$.*

The Legendre symbol helps us determining whether a is a quadratic residue.

Definition 2.7.2. *Let a be an integer and p be an odd prime. The Legendre symbol of a modulo p denoted by $\left(\frac{a}{p}\right)$ is defined as:*

$$\left(\frac{a}{p}\right) := \begin{cases} 1 \text{ if } p \nmid a \text{ and } a \text{ is a quadratic residue in } \mathbb{Z}/p\mathbb{Z}, \\ -1 \text{ if } p \nmid a \text{ and } a \text{ is not a quadratic residue in } \mathbb{Z}/p\mathbb{Z}, \\ 0 \text{ if } p \mid a. \end{cases}$$

The reason we ask for an odd prime is that every integer is a quadratic residue in $\mathbb{Z}/2\mathbb{Z}$. Because of that, we will be more interested in the congruence of a given integer in $\mathbb{Z}/8\mathbb{Z}$ where the only odd square is 1.

We recall some results on quadratic residues.

Theorem 2.7.3. *Let a and b be integers and let p be an odd prime number. We have that:*

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right).$$

Theorem 2.7.4 (Quadratic Reciprocity)**.** *Let p and q be distinct odd prime numbers. We have that:*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = \begin{cases} -1 & \text{if } p \equiv_4 q \equiv_4 3, \\ 1 & \text{otherwise.} \end{cases}$$

We add the following basic results to complement applications of Quadratic Reciprocity.

Lemma 2.7.5. *Let p be an odd prime, then:*

$$\left(\frac{-1}{p}\right) = \begin{cases} 1 & \text{if } p \equiv_4 1, \\ -1 & \text{otherwise.} \end{cases}$$

$$\left(\frac{2}{p}\right) = \begin{cases} 1 & \text{if } p \equiv_8 1 \text{ or } 7, \\ -1 & \text{otherwise.} \end{cases}$$

2.8. Other useful results from Number Theory

In this section, we gather some theorems that are not directly linked to the results of this thesis. However, they will play an important role in the background.

Theorem 2.8.1 (Chinese Remainder Theorem)**.** *Let $n_1,n_2,\ldots,n_k$ be integers relatively prime two by two. Let $a_1,a_2,\ldots,a_k$ be integers. Then there exists a unique integer $0 \leq x < \prod_{i=1}^{k} n_i$ such that $x \equiv_{n_i} a_i$ for $1 \leq i \leq k$.*

Theorem 2.8.2 (Dirichlet's Theorem on arithmetic progressions)**.** *Let a and n be relatively prime integers. Then there exist infinitely many primes congruent to $a(\text{mod } n)$.*

The two preceding results are important to guarantee that we never work with empty sets of primes when we ask for primes with certain congruences.

More precisely, for any prime p, we can guarantee the existence of infinitely many primes q such that $\left(\frac{p}{q}\right) = 1$ and infinitely many primes r such that $\left(\frac{r}{q}\right) = -1$. Also, with the Chinese Remainder Theorem, we can generalize this property to:

Lemma 2.8.3. *For any finite set of distinct primes* $\{p_1, \ldots, p_t\}$ *and given arbitrary* $\varepsilon_i \in \{-1,1\}$, *there exists infinitely many primes* q *such that:*

$$\begin{cases} \left(\dfrac{-1}{q}\right) & = \varepsilon_0, \\ \left(\dfrac{p_1}{q}\right) & = \varepsilon_1, \\ & \vdots \\ \left(\dfrac{p_t}{q}\right) & = \varepsilon_t. \end{cases}$$

We will also need the following theorem:

Theorem 2.8.4 (Hensel's Lemma)**.** *Let* f *be a polynomial with integer coefficients, let* x *be an integer, let* k *and* i *be positive integers and let* p *be a prime number. If* $f(x) \equiv_{p^k} 0$ *and* $f'(x) \not\equiv_p 0$, *then there exists an integer* y *such that* $y \equiv_{p^k} x$ *and* $f(y) \equiv_{p^{k+i}} 0$.

Hensel's Lemma will be very important for the proof of the necessary conditions for the construction of the matrix.

Chapter 3

Search for matrix conditions

3.1. Reduction on the number of cases

In this chapter, we will be looking for the necessary and sufficient conditions on (b_1,b_2) in order for the equation system

$$\begin{cases} b_1 z_1^2 - b_2 z_2^2 = e_2 d^2, & \text{(3.1.1a)} \\ b_1 z_1^2 - b_1 b_2 z_3^2 = e_3 d^2, & \text{(3.1.1b)} \\ b_2 z_2^2 - b_1 b_2 z_3^2 = (e_3 - e_2) d^2, & \text{(3.1.1c)} \end{cases}$$

to have a solution in $\mathbb{Q}_p$ for $p \in \mathcal{P} \cup \{\infty\}$. We recall that $b_1,b_2 \in \mathbb{Q}^*/(\mathbb{Q}^*)^2$ and can as such be seen as non-zero square-free integers.

The major problem in doing this is the massive number of possible cases. Indeed, for a given prime p, the conditions on (b_1,b_2) can change wildly depending on the values of $v_p(e_2)$, $v_p(e_3)$ and $v_p(e_3 - e_2)$.

In order to simplify this process, we will first reduce this problem as much as possible. There are three simple reduction steps that we can do on (e_2,e_3). These reduction steps are based on the fact that we are working on the elliptic curve $y^2 = x(x-e_2)(x-e_3)$ and that any change on the elliptic curve that does not change the nature of the group can also be done on the equation system.

We start by remarking that we can apply the transformations $x \mapsto \alpha^2 x$ and $y \mapsto \alpha^3 y$ with $\alpha \in \mathbb{Q}$. Using this, we can take α to be the common denominator of e_2 and e_3 in order to get that e_2 and e_3 are both integers.

Then, if a square β^2 divides both e_2 and e_3, we can take $\alpha = \frac{1}{\beta}$ in order to guarantee that the $GCD(e_2,e_3)$ is square-free.

Finally, we can apply the transformation $x \mapsto x + \gamma$ with $\gamma \in \mathbb{Q}$. Applying this transformation using the right constant γ allows us to choose which point of order 2 will be our e_2. Using this, we can reduce the number of cases in one p-adic field. As we will see later, the condition in $\mathbb{Q}_2$ are by far the most complicated. Because of this we will reduce the number of cases in $\mathbb{Q}_2$ by guaranteeing that $v_2(e_2) > v_2(e_3)$ and $v_2(e_2) > v_2(e_3 - e_2)$. This is always possible:

Lemma 3.1.1. *An elliptic curve in Legendre form $E : y^2 = x(x - e_2)(x - e_3)$ can always be reduced to an equation with $v_2(e_2) > v_2(e_3)$ and $v_2(e_2) > v_2(e_3 - e_2)$.*

Proof. From the second reduction, we have that $4 \nmid GCD(e_2,e_3)$.

It is not possible for all the three integers e_2, e_3 and $e_3 - e_2$ to all have different valuations. We remark that each of these integers can be obtained by adding or subtracting the other two. Indeed, if we name our three integers such that $v_2(a) < v_2(b) < v_2(c)$, we would have that $a = \pm(b \pm c)$. This would then imply that $v_2(a) \geq v_2(b)$ and this is a contradiction.

Since we now know that two of our three integers e_2, e_3 and $e_3 - e_2$ have the same valuation, we can guarantee that one of these integers has a strictly higher valuation than the other two. Indeed, if we let a and b respectively be the two integers with $v_2(a) = v_2(b)$, we would have that $v_2(c) > v_2(a)$ where c is the third integer since $c = \pm(a \pm b)$.

If e_2 has the highest valuation, we are done. If e_3 has the highest valuation, we can simply switch e_2 and e_3 in the elliptic curve. If $e_3 - e_2$ has the highest valuation, we simply use the transformation $x \mapsto x + e_3$ to get the elliptic curve $y^2 = x(x - (e_2 - e_3))(x - (-e_3))$ where $-(e_3 - e_2)$ is our new e_2. □

From now on, we will call the above three reductions *the conditions of Section 3.1.* To summarize, they are as follows:

(1) $e_2, e_3 \in \mathbb{Z}$,

(2) $GCD(e_2{,}e_3)$ is square-free,

(3) $v_2(e_2) > v_2(e_3)$.

3.2. Conditions in $\mathbb{R}$

The necessary and sufficient conditions for a solution in $\mathbb{R}$ are by far the easiest to determine. In fact, there are only three cases with only one condition each:

Theorem 3.2.1. *Equation System (3.1.1) has a non-trivial real solution if and only if the following conditions are satisfied:*

$$\begin{cases} e_2 > 0 \textit{ and } e_3 > 0 \implies b_1 > 0, \\ e_2 < 0 \textit{ and } e_3 - e_2 > 0 \implies b_2 > 0, \\ e_3 < 0 \textit{ and } e_3 - e_2 < 0 \implies b_1 b_2 > 0. \end{cases}$$

Proof. We start by remarking that, since the third equation in System (3.1.1) is the difference of the first two, showing that two of the equations have a simultaneous solution implies that the entire system has a solution. We then simply work case by case.

If $e_2 > 0$, $e_3 > 0$, $b_1 < 0$ and $b_2 > 0$, Equation (3.1.1a) has no real solution.

If $e_2 > 0$, $e_3 > 0$, $b_1 < 0$ and $b_2 < 0$, Equation (3.1.1b) has no real solution.

If $e_2 < 0$, $e_3 - e_2 > 0$, $b_1 > 0$ and $b_2 < 0$, Equation (3.1.1a) has no real solution.

If $e_2 < 0$, $e_3 - e_2 > 0$, $b_1 < 0$ and $b_2 < 0$, Equation (3.1.1c) has no real solution.

If $e_3 < 0$, $e_3 - e_2 < 0$, $b_1 > 0$ and $b_2 < 0$, Equation (3.1.1b) has no real solution.

If $e_3 < 0$, $e_3 - e_2 < 0$, $b_1 < 0$ and $b_2 > 0$, Equation (3.1.1c) has no real solution.

In all other cases, there are no sign problems so there are real solutions. For example, take z_3 either small or big enough in order for $\frac{e_3 d^2 + b_1 b_2 z_3^2}{b_1}$ and $\frac{(e_3 - e_2) d_2 + b_1 b_2 z_3^2}{b_2}$ to be positive. We can then take z_1 and z_2 to be their square roots to get a solution. □

3.3. Conditions in $\mathbb{Q}_2$

Since every term of Equation System (3.1.1) is of the same degree in the variables z_1, z_2, z_3 and d, looking for solutions to the system in $\mathbb{Q}_2$ is equivalent to looking for solutions in $\mathbb{Z}/2^k\mathbb{Z}$ for all k.

For any other prime, it is possible to work in $\mathbb{Z}/p\mathbb{Z}$ or $\mathbb{Z}/p^2\mathbb{Z}$ and then simply apply Hensel's lemma to get sufficient conditions in $\mathbb{Q}_p$. We will do this later when we work with odd primes. However, this strategy does not work with 2 because the derivative of a homogeneous equation of degree two is always 0 in $\mathbb{Z}/2\mathbb{Z}$. Because of this, the conditions in $\mathbb{Q}_2$ are considerably more complicated that those for $\mathbb{Q}_p$. This is why we reduced the number of cases in $\mathbb{Q}_2$ as much as possible by posing $v_2(e_2) > v_2(e_3)$.

Since the classical version of Hensel's lemma can not be applied for $\mathbb{Q}_2$, we will show that the conditions are necessary and sufficient in $\mathbb{Z}/2^k\mathbb{Z}$ for a k big enough by brute force and then do induction to show the sufficiency for all of $\mathbb{Q}_2$. One could use a more generalized version of Hensel's lemma to prove the necessity of the conditions. However, doing so would be more complex than the method used in this thesis.

Before starting, we remark that we can divide the equation system by common divisors. Because of this, we can assume that $GCD(z_1,z_2,z_3,d) = 1$. When working in $\mathbb{Q}_2$, it simply means that we can assume that not all our variables are even.

For the sake of simplicity, we will first give the conditions and then spend the rest of this section to prove them case by case.

3.3.1. The conditions for solvability in $\mathbb{Q}_2$

Before stating the conditions, we make some remarks.

Because of the generality of our elliptic curves, there are many cases to study and it might seem overwhelming. However, in most instances, only a few of the cases apply to a particular problem after the application of the reductions of Section 3.1. For example, in the congruent number problem, the only cases that apply are those with $v_2(e_2) = 1$ and $v_2(e_3) = 0$ or those with $v_2(e_2) = 2$ and $v_2(e_3) = 1$ since the related elliptic curve can be written in Legendre form with $e_2 = -2n$ and

$e_3 = n$ where n is square-free. We aim to study all the cases so that we can provide conditions for any possible problem of this type.

Also, when working in $\mathbb{Q}_2$, the classical version Hensel's lemma does not apply since the derivative of a homogeneous second degree equation is always 0. This makes the cases in $\mathbb{Q}_2$ very irregular and that produces a vast number of conditions. However, once $v_2(e_2)$ becomes large enough, we will be able to reduce the cases to a smaller valuation of e_2 so there is a finite number of cases.

We gather all the conditions in four tables that will be presented in the following pages. We remark that for given e_2 and e_3, we have three conditions in each cell of the tables. Sometimes it seems that there are only two conditions, but this is caused by an implicit condition. Indeed, when there seems to be only two conditions, it is because either we have the added condition that $2 \nmid b_1$ that gives us the "No solution" case or one of the conditions is $x \equiv_8 1$ that can be seen as $x \equiv_8 1$ or 7 and $x \equiv_4 1$ simultaneously. We will come back to this when we transform the conditions into matrix lines.

Theorem 3.3.1. *If $8 \nmid e_2$ and $2 \nmid e_3$, the following conditions are necessary and sufficient for Equation System (3.1.1) to have a non-trivial solution in $\mathbb{Q}_2$:*

		If $v_2(e_2) = 1$:		*If $v_2(e_2) = 2$:*	
		If $2 \nmid b_1$:	*If $2 \mid b_1$:*	*If $2 \nmid b_1$:*	*If $2 \mid b_1$:*
If $\overline{e_2} \equiv_4 1$:	*If $\overline{e_3} \equiv_8 1$:*	$2 \nmid b_2$, $\overline{b_1} \equiv_4 1$, $\overline{b_1 b_2} \equiv_8$ *1 or 7.*	$2 \mid b_2$, $\overline{b_1} \equiv_4 1$, $\overline{b_1 b_2} \equiv_8$ *1 or 7.*	$2 \nmid b_2$, $\overline{b_1} \equiv_4 1$.	*No solution.*
	If $\overline{e_3} \equiv_8 5$:	$2 \nmid b_2$, $\overline{b_1} \equiv_4 1$, $\overline{b_1 b_2} \equiv_8$ *1 or 7.*	$2 \mid b_2$, $\overline{b_1} \equiv_4 1$, $\overline{3 b_1 b_2} \equiv_8$ *1 or 7.*	$2 \nmid b_2$, $\overline{b_1} \equiv_4 1$.	*No solution.*
	If $\overline{e_3} \equiv_8 3$:	$2 \nmid b_2$, $\overline{b_2} \equiv_4 1$, $\overline{b_1 b_2} \equiv_8$ *1 or 3.*	$2 \mid b_2$, $\overline{-b_2} \equiv_4 1$, $\overline{-b_1 b_2} \equiv_8$ *1 or 3.*	$2 \nmid b_2$, $\overline{b_1} \equiv_8$ *1 or 7* $\iff$ $\overline{b_2} \equiv_8$ *1 or 3,* $\overline{b_1 b_2} \equiv_4 1$.	$2 \mid b_2$, $\overline{b_1} \equiv_8$ *1 or 7* $\iff$ $\overline{-b_2} \equiv_8$ *1 or 3,* $\overline{-b_1 b_2} \equiv_4 1$.
	If $\overline{e_3} \equiv_8 7$:	$2 \nmid b_2$, $\overline{b_2} \equiv_4 1$, $\overline{b_1 b_2} \equiv_8$ *1 or 3.*	$2 \mid b_2$, $\overline{-b_2} \equiv_4 1$, $\overline{b_1 b_2} \equiv_8$ *1 or 3.*	$2 \nmid b_2$, $\overline{b_1 b_2} \equiv_4 1$.	*No solution.*
If $\overline{e_2} \equiv_4 3$:	*If $\overline{e_3} \equiv_8 1$:*	$2 \nmid b_2$, $\overline{b_1} \equiv_4 1$, $\overline{b_1 b_2} \equiv_8$ *1 or 3.*	$2 \mid b_2$, $\overline{-b_1} \equiv_4 1$, $\overline{-b_1 b_2} \equiv_8$ *1 or 3.*	$2 \nmid b_2$, $\overline{b_2} \equiv_4 1$.	*No solution.*
	If $\overline{e_3} \equiv_8 5$:	$2 \nmid b_2$, $\overline{b_1} \equiv_4 1$, $\overline{b_1 b_2} \equiv_8$ *1 or 3.*	$2 \mid b_2$, $\overline{-b_1} \equiv_4 1$, $\overline{b_1 b_2} \equiv_8$ *1 or 3.*	$2 \nmid b_2$, $\overline{b_2} \equiv_4 1$.	*No solution.*
	If $\overline{e_3} \equiv_8 3$:	$2 \nmid b_2$, $\overline{b_2} \equiv_4 1$, $\overline{b_1 b_2} \equiv_8$ *1 or 7.*	$2 \mid b_2$, $\overline{b_2} \equiv_4 1$, $\overline{3 b_1 b_2} \equiv_8$ *1 or 7.*	$2 \nmid b_2$, $\overline{b_1 b_2} \equiv_4 1$.	*No solution.*
	If $\overline{e_3} \equiv_8 7$:	$2 \nmid b_2$, $\overline{b_2} \equiv_4 1$, $\overline{b_1 b_2} \equiv_8$ *1 or 7.*	$2 \mid b_2$, $\overline{b_2} \equiv_4 1$, $\overline{b_1 b_2} \equiv_8$ *1 or 7.*	$2 \nmid b_2$, $\overline{b_1} \equiv_8$ *1 or 7* $\iff$ $\overline{b_2} \equiv_8$ *1 or 3,* $\overline{b_1 b_2} \equiv_4 1$.	$2 \mid b_2$, $\overline{b_1} \equiv_8$ *1 or 7* $\iff$ $\overline{b_2} \equiv_8$ *1 or 3,* $\overline{-b_1 b_2} \equiv_4 1$.

Table 3.1. Conditions for a solution in $\mathbb{Q}_2$ when $8 \nmid e_2$ and $2 \nmid e_3$.

Theorem 3.3.2. *If $3 \leq v_2(e_2) \leq 4$ and $2 \nmid e_3$, the following conditions are necessary and sufficient for Equation System (3.1.1) to have a non-trivial solution in $\mathbb{Q}_2$:*

		If $v_2(e_2) = 3$*:*		*If* $v_2(e_2) = 4$*:*	
		If $2 \nmid b_1$*:*	*If* $2 \mid b_1$*:*	*If* $2 \nmid b_1$*:*	*If* $2 \mid b_1$*:*
If $\overline{e_2} \equiv_4 1$*:*	*If* $\overline{e_3} \equiv_8 1$*:*	$2 \nmid b_2$, $\overline{b_2} \equiv_4 1$, $\overline{b_1 b_2} \equiv_8$ *1 or 3.*	$2 \mid b_2$, $\overline{-b_2} \equiv_4 1$, $\overline{-b_1 b_2} \equiv_8$ *1 or 3.*	$2 \nmid b_2$, $\overline{b_1} \equiv_4 1$, $\overline{b_1 b_2} \equiv_8$ *1 or 7.*	$2 \mid b_2$, $\overline{b_1} \equiv_4 1$, $\overline{b_1 b_2} \equiv_8$ *1 or 7.*
	If $\overline{e_3} \equiv_8 5$*:*	$2 \nmid b_2$, $\overline{b_1} \equiv_4 1$, $\overline{b_1 b_2} \equiv_8$ *1 or 7.*	$2 \mid b_2$, $\overline{b_1} \equiv_4 1$, $\overline{3 b_1 b_2} \equiv_8$ *1 or 7.*	$2 \nmid b_2$, $\overline{b_1} \equiv_4 1$, $\overline{b_1 b_2} \equiv_8$ *1 or 3.*	$2 \mid b_2$, $\overline{-b_1} \equiv_4 1$, $\overline{b_1 b_2} \equiv_8$ *1 or 3.*
	If $\overline{e_3} \equiv_8 3$*:*	$2 \nmid b_2$, $\overline{b_1 b_2} \equiv_8 1$.	$2 \mid b_2$, $\overline{5 b_1 b_2} \equiv_8 1$.	$2 \nmid b_2$, $\overline{b_1 b_2} \equiv_4 1$.	*No solution.*
	If $\overline{e_3} \equiv_8 7$*:*	$2 \nmid b_2$, $\overline{b_1 b_2} \equiv_8 1$.	$2 \mid b_2$, $\overline{b_1 b_2} \equiv_8 1$.	$2 \nmid b_2$, $\overline{b_1 b_2} \equiv_4 1$.	*No solution.*
If $\overline{e_2} \equiv_4 3$*:*	*If* $\overline{e_3} \equiv_8 1$*:*	$2 \nmid b_2$, $\overline{b_1} \equiv_4 1$, $\overline{b_1 b_2} \equiv_8$ *1 or 3.*	$2 \mid b_2$, $\overline{-b_1} \equiv_4 1$, $\overline{-b_1 b_2} \equiv_8$ *1 or 3.*	$2 \nmid b_2$, $\overline{b_2} \equiv_4 1$, $\overline{b_1 b_2} \equiv_8$ *1 or 7.*	$2 \mid b_2$, $\overline{b_2} \equiv_4 1$, $\overline{b_1 b_2} \equiv_8$ *1 or 7.*
	If $\overline{e_3} \equiv_8 5$*:*	$2 \nmid b_2$, $\overline{b_2} \equiv_4 1$, $\overline{b_1 b_2} \equiv_8$ *1 or 7.*	$2 \mid b_2$, $\overline{b_2} \equiv_4 1$, $\overline{3 b_1 b_2} \equiv_8$ *1 or 7.*	$2 \nmid b_2$, $\overline{b_2} \equiv_4 1$, $\overline{b_1 b_2} \equiv_8$ *1 or 3.*	$2 \mid b_2$, $\overline{-b_2} \equiv_4 1$, $\overline{b_1 b_2} \equiv_8$ *1 or 3.*
	If $\overline{e_3} \equiv_8 3$*:*	$2 \nmid b_2$, $\overline{b_1 b_2} \equiv_8 1$.	$2 \mid b_2$, $\overline{5 b_1 b_2} \equiv_8 1$.	$2 \nmid b_2$, $\overline{b_1 b_2} \equiv_4 1$.	*No solution.*
	If $\overline{e_3} \equiv_8 7$*:*	$2 \nmid b_2$, $\overline{b_1 b_2} \equiv_8 1$.	$2 \mid b_2$, $\overline{b_1 b_2} \equiv_8 1$.	$2 \nmid b_2$, $\overline{b_1 b_2} \equiv_4 1$.	*No solution.*

Table 3.2. Conditions for a solution in $\mathbb{Q}_2$ when $3 \leq v_2(e_2) \leq 4$ and $2 \nmid e_3$.

Theorem 3.3.3. *If* $32 \mid e_2$ *and* $2 \nmid e_3$*, the following conditions are necessary and sufficient for Equation System (3.1.1) to have a non-trivial solution in* $\mathbb{Q}_2$*:*

		If $v_2(e_2) \equiv_2 1$*:*		*If* $v_2(e_2) \equiv_2 0$*:*	
		If $2 \nmid b_1$*:*	*If* $2 \mid b_1$*:*	*If* $2 \nmid b_1$*:*	*If* $2 \mid b_1$*:*
If $\overline{e_2} \equiv_4 1$*:*	*If* $\overline{e_3} \equiv_8 1$*:*	$2 \nmid b_2$, $\overline{b_1} \equiv_4 1$, $\overline{b_1 b_2} \equiv_8$ *1 or 7.*	$2 \mid b_2$, $\overline{b_1} \equiv_4 1$, $\overline{b_1 b_2} \equiv_8$ *1 or 7.*	$2 \nmid b_2$, $\overline{b_1} \equiv_4 1$, $\overline{b_1 b_2} \equiv_8$ *1 or 7.*	$2 \mid b_2$, $\overline{b_1} \equiv_4 1$, $\overline{b_1 b_2} \equiv_8$ *1 or 7.*
	If $\overline{e_3} \equiv_8 5$*:*	$2 \nmid b_2$, $\overline{b_2} \equiv_4 1$, $\overline{b_1 b_2} \equiv_8$ *1 or 3.*	$2 \mid b_2$, $\overline{-b_2} \equiv_4 1$, $\overline{b_1 b_2} \equiv_8$ *1 or 3.*	$2 \nmid b_2$, $\overline{b_1} \equiv_4 1$, $\overline{b_1 b_2} \equiv_8$ *1 or 3.*	$2 \mid b_2$, $\overline{-b_1} \equiv_4 1$, $\overline{b_1 b_2} \equiv_8$ *1 or 3.*
	If $\overline{e_3} \equiv_8 3$*:*	$2 \nmid b_2$, $\overline{b_1 b_2} \equiv_8 1$.	$2 \mid b_2$, $\overline{5 b_1 b_2} \equiv_8 1$.	$2 \nmid b_2$, $\overline{b_1 b_2} \equiv_4 1$.	*No solution.*
	If $\overline{e_3} \equiv_8 7$*:*	$2 \nmid b_2$, $\overline{b_1 b_2} \equiv_8 1$.	$2 \mid b_2$, $\overline{b_1 b_2} \equiv_8 1$.	$2 \nmid b_2$, $\overline{b_1 b_2} \equiv_8 1$.	$2 \mid b_2$, $\overline{b_1 b_2} \equiv_8 1$.
If $\overline{e_2} \equiv_4 3$*:*	*If* $\overline{e_3} \equiv_8 1$*:*	$2 \nmid b_2$, $\overline{b_2} \equiv_4 1$, $\overline{b_1 b_2} \equiv_8$ *1 or 7.*	$2 \mid b_2$, $\overline{b_2} \equiv_4 1$, $\overline{b_1 b_2} \equiv_8$ *1 or 7.*	$2 \nmid b_2$, $\overline{b_2} \equiv_4 1$, $\overline{b_1 b_2} \equiv_8$ *1 or 7.*	$2 \mid b_2$, $\overline{b_2} \equiv_4 1$, $\overline{b_1 b_2} \equiv_8$ *1 or 7.*
	If $\overline{e_3} \equiv_8 5$*:*	$2 \nmid b_2$, $\overline{b_1} \equiv_4 1$, $\overline{b_1 b_2} \equiv_8$ *1 or 3.*	$2 \mid b_2$, $\overline{-b_1} \equiv_4 1$, $\overline{b_1 b_2} \equiv_8$ *1 or 3.*	$2 \nmid b_2$, $\overline{b_2} \equiv_4 1$, $\overline{b_1 b_2} \equiv_8$ *1 or 3.*	$2 \mid b_2$, $\overline{-b_2} \equiv_4 1$, $\overline{b_1 b_2} \equiv_8$ *1 or 3.*
	If $\overline{e_3} \equiv_8 3$*:*	$2 \nmid b_2$, $\overline{b_1 b_2} \equiv_8 1$.	$2 \mid b_2$, $\overline{5 b_1 b_2} \equiv_8 1$.	$2 \nmid b_2$, $\overline{b_1 b_2} \equiv_4 1$.	*No solution.*
	If $\overline{e_3} \equiv_8 7$*:*	$2 \nmid b_2$, $\overline{b_1 b_2} \equiv_8 1$.	$2 \mid b_2$, $\overline{b_1 b_2} \equiv_8 1$.	$2 \nmid b_2$, $\overline{b_1 b_2} \equiv_8 1$.	$2 \mid b_2$, $\overline{b_1 b_2} \equiv_8 1$.

Table 3.3. Conditions for a solution in $\mathbb{Q}_2$ when $32 \mid e_2$ and $2 \nmid e_3$.

Theorem 3.3.4. *If $2 \mid e_3$, the following conditions are necessary and sufficient for Equation System (3.1.1) to have a non-trivial solution in $\mathbb{Q}_2$:*

			If $v_2(e_2) = 2$:	*If $v_2(e_2) = 3$*	*If $16 \mid e_2$ and $v_2(e_2) \equiv_2 0$:*	*If $16 \mid e_2$ and $v_2(e_2) \equiv_2 1$:*
If $\overline{e_3} \equiv_4 1$:	*If $2 \nmid b_1$:*	*If $2 \nmid b_2$:*	$\overline{b_1} \equiv_8 1 \text{ or } 7,$ $\overline{b_2} \equiv_8 1 \text{ or } 3,$ $\overline{b_1b_2} \equiv_4 1.$	$\overline{b_1} \equiv_8 1 \text{ or } 3,$ $\overline{b_2} \equiv_8 1 \text{ or } 3,$ $\overline{b_1b_2} \equiv_4 1.$	$\overline{b_1} \equiv_8 1 \text{ or } 3,$ $\overline{b_2} \equiv_8 1 \text{ or } 3,$ $\overline{b_1b_2} \equiv_4 1.$	$\overline{b_1} \equiv_8 1 \text{ or } 3,$ $\overline{b_2} \equiv_8 1 \text{ or } 3,$ $\overline{b_1b_2} \equiv_4 1.$
		If $2 \mid b_2$:	$\overline{b_1e_2} \equiv_8 1 \text{ or } 7,$ $\overline{-b_2e_2(e_3 - e_2)} \equiv_8 1 \text{ or } 3,$ $\overline{b_1b_2} \equiv_4 1.$	$\overline{b_1e_2e_3} \equiv_8 1 \text{ or } 3,$ $\overline{-b_2e_2} \equiv_8 1 \text{ or } 3,$ $\overline{-b_1b_2} \equiv_4 1.$	$\overline{b_1e_2} \equiv_8 1 \text{ or } 3,$ $\overline{-b_2e_2e_3} \equiv_8 1 \text{ or } 3,$ $\overline{-b_1b_2} \equiv_4 1.$	$\overline{b_1e_2e_3} \equiv_8 1 \text{ or } 3,$ $\overline{-b_2e_2} \equiv_8 1 \text{ or } 3,$ $\overline{-b_1b_2} \equiv_4 1.$
	If $2 \mid b_1$:	*If $2 \nmid b_2$:*	$\overline{b_1e_2e_3} \equiv_8 1 \text{ or } 7,$ $\overline{-b_2e_2} \equiv_8 1 \text{ or } 3,$ $\overline{-b_1b_2} \equiv_4 1.$	$\overline{b_1e_2} \equiv_8 1 \text{ or } 3,$ $\overline{b_2e_2e_3} \equiv_8 1 \text{ or } 3,$ $\overline{-b_1b_2} \equiv_4 1.$	$\overline{b_1e_2e_3} \equiv_8 1 \text{ or } 3,$ $\overline{-b_2e_2} \equiv_8 1 \text{ or } 3,$ $\overline{-b_1b_2} \equiv_4 1.$	$\overline{b_1e_2} \equiv_8 1 \text{ or } 3,$ $\overline{-b_2e_2e_3} \equiv_8 1 \text{ or } 3,$ $\overline{-b_1b_2} \equiv_4 1.$
		If $2 \mid b_2$:	$\overline{b_1e_3} \equiv_8 1 \text{ or } 7,$ $\overline{b_2(e_3 - e_2)} \equiv_8 1 \text{ or } 3,$ $\overline{-b_1b_2} \equiv_4 1.$	$\overline{b_1e_3} \equiv_8 1 \text{ or } 3,$ $\overline{-b_2e_3} \equiv_8 1 \text{ or } 3,$ $\overline{b_1b_2} \equiv_4 1.$	$\overline{b_1e_3} \equiv_8 1 \text{ or } 3,$ $\overline{b_2e_3} \equiv_8 1 \text{ or } 3,$ $\overline{b_1b_2} \equiv_4 1.$	$\overline{b_1e_3} \equiv_8 1 \text{ or } 3,$ $\overline{b_2e_3} \equiv_8 1 \text{ or } 3,$ $\overline{b_1b_2} \equiv_4 1.$
If $\overline{e_3} \equiv_4 3$:	*If $2 \nmid b_1$:*	*If $2 \nmid b_2$:*	$\overline{b_1} \equiv_8 1 \text{ or } 3,$ $\overline{b_2} \equiv_8 1 \text{ or } 7,$ $\overline{b_1b_2} \equiv_4 1.$	$\overline{b_1} \equiv_8 1 \text{ or } 7,$ $\overline{b_2} \equiv_8 1 \text{ or } 7,$ $\overline{b_1b_2} \equiv_4 1.$	$\overline{b_1} \equiv_8 1 \text{ or } 7,$ $\overline{b_2} \equiv_8 1 \text{ or } 7,$ $\overline{b_1b_2} \equiv_4 1.$	$\overline{b_1} \equiv_8 1 \text{ or } 7,$ $\overline{b_2} \equiv_8 1 \text{ or } 7,$ $\overline{b_1b_2} \equiv_4 1.$
		If $2 \mid b_2$:	$\overline{b_1e_2} \equiv_8 1 \text{ or } 3,$ $\overline{b_2e_2(e_3 - e_2)} \equiv_8 1 \text{ or } 7,$ $\overline{-b_1b_2} \equiv_4 1.$	$\overline{b_1e_2e_3} \equiv_8 1 \text{ or } 7,$ $\overline{b_2e_2} \equiv_8 1 \text{ or } 7,$ $\overline{b_1b_2} \equiv_4 1.$	$\overline{b_1e_2} \equiv_8 1 \text{ or } 7,$ $\overline{b_2e_2e_3} \equiv_8 1 \text{ or } 7,$ $\overline{b_1b_2} \equiv_4 1.$	$\overline{b_1e_2e_3} \equiv_8 1 \text{ or } 7,$ $\overline{b_2e_2} \equiv_8 1 \text{ or } 7,$ $\overline{b_1b_2} \equiv_4 1.$
	If $2 \mid b_1$:	*If $2 \nmid b_2$:*	$\overline{b_1e_2e_3} \equiv_8 1 \text{ or } 3,$ $\overline{b_2e_2} \equiv_8 1 \text{ or } 7,$ $\overline{b_1b_2} \equiv_4 1.$	$\overline{b_1e_2} \equiv_8 1 \text{ or } 7,$ $\overline{3b_2e_2e_3} \equiv_8 1 \text{ or } 7,$ $\overline{b_1b_2} \equiv_4 1.$	$\overline{b_1e_2e_3} \equiv_8 1 \text{ or } 7,$ $\overline{b_2e_2} \equiv_8 1 \text{ or } 7,$ $\overline{b_1b_2} \equiv_4 1.$	$\overline{b_1e_2} \equiv_8 1 \text{ or } 7,$ $\overline{b_2e_2e_3} \equiv_8 1 \text{ or } 7,$ $\overline{b_1b_2} \equiv_4 1.$
		If $2 \mid b_2$:	$\overline{b_1e_3} \equiv_8 1 \text{ or } 3,$ $\overline{b_2(e_3 - e_2)} \equiv_8 1 \text{ or } 7,$ $\overline{-b_1b_2} \equiv_4 1.$	$\overline{b_1e_3} \equiv_8 1 \text{ or } 7,$ $\overline{3b_2e_3} \equiv_8 1 \text{ or } 7,$ $\overline{b_1b_2} \equiv_4 1.$	$\overline{b_1e_3} \equiv_8 1 \text{ or } 7,$ $\overline{b_2e_3} \equiv_8 1 \text{ or } 7,$ $\overline{b_1b_2} \equiv_4 1.$	$\overline{b_1e_3} \equiv_8 1 \text{ or } 7,$ $\overline{b_2e_3} \equiv_8 1 \text{ or } 7,$ $\overline{b_1b_2} \equiv_4 1.$

Table 3.4. Conditions for a solution in $\mathbb{Q}_2$ when $2 \mid e_3$.

3.3.2. The proofs of necessity

We separate the proofs that our conditions are necessary from the proofs that they are sufficient. There are two main reasons for that. The first reason is that both types of proofs are very different. However the proofs of necessity are very similar to each other and the same is true for the proofs of sufficiency. It is therefore natural, in a classification mindset, to separate the two types of proofs. The second reason is that we only really need for the conditions to be necessary for most of the results that we obtain in this thesis. The proofs of sufficiency are here to show that there are no other local conditions that we could have added to get new results. The proofs of sufficiency could also be used to find the exact elliptic curve rank if one were able to calculate the size of the Tate-Shafarevich group.

With that in mind, we will write the proofs of necessity in this section. For small valuations, we remark that the conditions under consideration are necessary for a solution in $\mathbb{Z}/2^n\mathbb{Z}$ with a small enough n. In these cases, we simply apply brute force and check all possibilities using a Python program. An algorithm that does it in an acceptable time (it is still somewhat long for some of the valuations) is given in Appendix A.

Proposition 3.3.5. *If $2 \nmid e_3$, $v_2(e_2) \leq 4$ and Equation System (3.1.1) has a non trivial solution in $\mathbb{Q}_2$, then b_1 and b_2 respect the conditions of Theorems 3.3.1 and 3.3.2.*

If $2 \mid e_3$, $v_2(e_2) \leq 3$ and Equation System (3.1.1) has a non trivial solution in $\mathbb{Q}_2$, then b_1 and b_2 respect the conditions of Theorem 3.3.4.

Proof. When $2 \nmid e_3$ and $v_2(e_2) = 1$, it can be verified, using the algorithm given in Appendix A, that the conditions of Theorem 3.3.1 are necessary for a solution in $\mathbb{Z}/32\mathbb{Z}$.

When $2 \nmid e_3$ and $v_2(e_2) = 2$, it can be verified, using the algorithm given in Appendix A, that the conditions of Theorem 3.3.1 are necessary for a solution in $\mathbb{Z}/64\mathbb{Z}$.

When $2 \nmid e_3$ and $v_2(e_2) = 3$, it can be verified, using the algorithm given in Appendix A, that the conditions of Theorem 3.3.2 are necessary for a solution in $\mathbb{Z}/128\mathbb{Z}$.

When $2 \nmid e_3$ and $v_2(e_2) = 4$, it can be verified, using the algorithm given in Appendix A, that the conditions of Theorem 3.3.2 are necessary for a solution in $\mathbb{Z}/256\mathbb{Z}$.

When $2 \mid e_3$ and $v_2(e_2) = 2$, it can be verified, using the algorithm given in Appendix A, that the conditions of Theorem 3.3.4 are necessary for a solution in $\mathbb{Z}/32\mathbb{Z}$.

When $2 \mid e_3$ and $v_2(e_2) = 3$, it can be verified, using the algorithm given in Appendix A, that the conditions of Theorem 3.3.4 are necessary for a solution in $\mathbb{Z}/64\mathbb{Z}$. □

The rest of the cases have an indeterminate valuation and this implies that a simple brute force proof would not work.

The conditions can be separated in multiple cases. We will organize the cases in lemmas.

3.3.2.1. Proofs when $32 \mid e_2$, $v_2(e_2) \equiv_2 1$ and $2 \nmid e_3$:

Lemma 3.3.6. *If Equation System (3.1.1) has a non trivial solution in $\mathbb{Q}_2$, then:*

$$2 \mid b_1 \iff 2 \mid b_2.$$

Proof. Recall that b_1,$b_2 \in \mathbb{Q}(S,2)$. Because of this b_1 and b_2 are represented by square-free integers. This fact will be important for almost all proofs of this chapter. For this particular proof, it implies that $4 \nmid b_1$,b_2.

We proceed by contradiction. If $2 \mid b_1$ and $2 \nmid b_2$, Equation (3.1.1b) implies that $2 \mid d$, then Equation (3.1.1a) implies that $2 \mid z_2$, then Equation (3.1.1c) implies that $2 \mid z_3$ (since $4 \nmid b_1$) and Equation (3.1.1a) implies that $2 \mid z_1$ (since $4 \nmid b_1$) and this is a contradiction since $GCD(z_1,z_2,z_3,d) = 1$.

If $2 \nmid b_1$ and $2 \mid b_2$, Equation (3.1.1c) implies that $2 \mid d$, then Equation (3.1.1a) implies that $2 \mid z_1$, then Equation (3.1.1b) implies that $2 \mid z_3$ (since $4 \nmid b_2$) and Equation (3.1.1a) implies that $2 \mid z_2$ (since $4 \nmid b_2$) and this is another contradiction. □

Lemma 3.3.7. *If $\overline{e_3} \equiv_4 3$ and Equation System (3.1.1) has a non trivial solution in $\mathbb{Q}_2$, then:*

$$\begin{cases} 2 \nmid b_1 \implies \overline{b_1 b_2} \equiv_8 1, \\ 2 \mid b_1 \implies -\overline{b_1 b_2}\overline{e_3} \equiv_8 1. \end{cases}$$

Proof. We separate the proof in two cases depending on the parity of b_1. Recall that Lemma 3.3.6 implies that b_1 and b_2 have the same parity.

If $2 \nmid b_1$, we consider several subcases depending on the 2-valuations of z_1 and z_2. Remark that evaluating Equation (3.1.1a) modulo 8 implies that $2 \mid z_1 \iff 2 \mid z_2$ since the equation becomes $b_1 z_1^2 - b_2 z_2^2 \equiv_8 0$. We can repeat this argument and evaluate Equation (3.1.1a) modulo 2^{1+2i} in order to show that $2^i \mid z_1 \iff 2^i \mid z_2$ for $i \leq \frac{v_2(e_2)-1}{2}$.

If $2 \nmid z_1 z_2$, Equation (3.1.1a) modulo 8 becomes $b_1 - b_2 \equiv_8 0$ and this implies that $b_1 b_2 \equiv_8 1$.

If $2 \mid z_1, z_2$, Equation (3.1.1b) implies that $2 \mid z_3 \iff 2 \mid d$ since $2 \nmid b_1 b_2 e_3$. In order for z_1, z_2, z_3, and d to have no common factor, $2 \nmid z_3 d$. We will use this property for the next subcases.

If $2 \mid z_1, z_2$ but $2^{(v_2(e_2)-1)/2} \nmid z_1, z_2$, evaluating Equation (3.1.1a) modulo $2^{v_2(e_2)}$ implies that $b_1 - b_2 \equiv_8 0$ and then that $b_1 b_2 \equiv_8 1$.

If $2^{(v_2(e_2)-1)/2} \mid\mid z_1, z_2$, evaluating Equation (3.1.1b) modulo 4 implies that $-b_1 b_2 \equiv_4 e_3 \equiv_4 3$. This means that $b_1 \equiv_4 b_2$. However, evaluating Equation (3.1.1a) modulo $2^{v_2(e_2)+1}$ implies that $b_1 - b_2 \equiv_4 2$. This is impossible since $b_1 \equiv_4 b_2$ implies that $b_1 - b_2 \equiv_4 0$.

If $2^{(v_2(e_2)+1)/2} \mid z_1, z_2$, Equation (3.1.1a) has no solution since it would imply that $v_2(b_1 z_1^2 - b_2 z_2^2) > v_2(e_2 d^2)$.

This concludes the case when $2 \nmid b_1$.

If $2 \mid b_1$, we again consider several subcases depending on the 2-valuations of z_1 and z_2. This time, we check the 2-valuations of the terms in Equation (3.1.1b) to remark that $2 \mid d$ and then that $2 \mid z_1$. Doing the same with Equation (3.1.1c) implies that $2 \mid z_2$. This then means that $2 \nmid z_3$ since $GCD(z_1, z_2, z_3, d) = 1$. Knowing this, the 2-valuations of the terms of Equation (3.1.1c) imply that $4 \nmid d$ because $8 \nmid b_1 b_2 z_3^2$.

If $4 \nmid z_1$,z_2, Equation (3.1.1a) implies that $b_1b_2 \equiv_8 1$. However, evaluating Equation (3.1.1b) modulo 16 implies that $b_1 - \overline{b_1b_2} \equiv_4 e_3$ and this then implies that $2 - 1 \equiv_4 3$ which is false. This means that $4 \mid z_1$ or $4 \mid z_2$.

If $4 \mid z_1$ or $4 \mid z_2$, Equation(3.1.1a) implies that 4 must also divide the other using the same reasoning used when $2 \nmid b_1$. Equation (3.1.1b) then implies that $-\overline{b_1b_2} \equiv_8 \overline{e_3}$ when evaluated modulo 32. This is equivalent to $-\overline{b_1b_2}\overline{e_3} \equiv_8 1$.

This concludes the case when $2 \mid b_1$.

□

Lemma 3.3.8. *If $\overline{e_3} \equiv_8 1$ and Equation System (3.1.1) has a non trivial solution in $\mathbb{Q}_2$, then:*

$$\overline{b_1b_2} \equiv_8 1 \textit{ or } 7.$$

Proof. We separate the proof in two cases depending on the parity of b_1. Recall that Lemma 3.3.6 implies that b_1 and b_2 have the same parity.

If $2 \nmid b_1$, we consider several subcases depending on the 2-valuations of z_1 and z_2. Recall that evaluating Equation (3.1.1a) modulo 8 implies that $2 \mid z_1 \iff 2 \mid z_2$. For the same reason, $4 \mid z_1 \iff 4 \mid z_2$.

If $2 \nmid z_1z_2$, then $z_1^2 \equiv_8 z_2^2 \equiv_8 1$. This implies that $b_1 \equiv_8 b_2$ and then that $b_1b_2 \equiv_8 1$.

If $2 \mid z_1$,z_2, Equation (3.1.1b) implies that $2 \mid z_3 \iff 2 \mid d$ since $2 \nmid b_1b_2e_3$. In order for z_1, z_2, z_3, and d to have no common factor, $2 \nmid z_3d$. We will use this property for the next subcases.

If $2 \mid\mid z_1$,z_2, Equation (3.1.1b) modulo 8 becomes $4 - b_1b_2 \equiv_8 1$ and this implies that $b_1b_2 \equiv_8 3$. However, Equation (3.1.1a) modulo 16 becomes $b_1 - b_2 \equiv_4 0$ after we divide every term by 4. This would imply that $b_1b_2 \equiv_4 1$ and it would be a contradiction. This case is then impossible.

If $4 \mid z_1$,z_2, Equation (3.1.1b) modulo 8 is $-b_1b_2 \equiv_8 1$ and this implies that $b_1b_2 \equiv_8 7$.

This concludes the case when $2 \nmid b_1$.

If $2 \mid b_1$, Equation (3.1.1b) modulo 2 implies that $2 \mid d$. We then reevaluate it modulo 4 to remark that $2 \mid z_1$. We can also evaluate Equation (3.1.1c) modulo 4 to remark that $2 \mid z_2$. Since $GCD(z_1,z_2,z_3,d) = 1$, this implies that $2 \nmid z_3$. Equation (3.1.1b) modulo 8 becomes $b_1b_2 \equiv_8 d^2$ and implies that $4 \nmid d$. With all this information, we consider two subcases depending on the 2-valuations of z_1 and z_2.

If $4 \mid z_1$ or $4 \mid z_2$, Equation (3.1.1b) or Equation (3.1.1c) respectively implies that $b_1b_2 \equiv_{32} d^2$. Dividing the equation by 4 the implies that $-\overline{b_1b_2} \equiv_8 1$ and this is equivalent to $\overline{b_1b_2} \equiv_8 7$.

If $4 \nmid z_1,z_2$, Equation (3.1.1a) evaluated modulo 32 becomes $\overline{b_1} - \overline{b_2} \equiv_8 0$ when divided by 4. This implies that $\overline{b_1b_2} \equiv_8 1$.

This concludes the case when $2 \mid b_1$.

□

Lemma 3.3.9. *If $\overline{e_3} \equiv_8 5$ and Equation System (3.1.1) has a non trivial solution in $\mathbb{Q}_2$, then:*

$$\overline{b_1b_2} \equiv_8 1 \textit{ or } 3.$$

Proof. The proof of this lemma is practically identical to the proof of Lemma 3.3.8, the only difference being the right side of Equations (3.1.1b) and (3.1.1c). □

Lemma 3.3.10. *If $\overline{e_2} \equiv_4 1$, $\overline{e_3} \equiv_8 1$ and Equation System (3.1.1) has a non trivial solution in $\mathbb{Q}_2$, then:*

$$\overline{b_1} \equiv_4 1.$$

Proof. We separate the problem in two cases depending on the parity of b_1. Recall that Lemma 3.3.6 implies that b_1 and b_2 have the same parity. Each case will then be separated into subcases depending on the 2-valuations of z_1 and z_2.

If $2 \nmid b_1$:

If $2 \nmid z_1z_2$, Equation (3.1.1a) evaluated modulo 4 implies that $b_1 \equiv_4 b_2$. Applying this to Equation (3.1.1b) implies that $b_1 - z_3^2 \equiv_4 d^2$. The only solution to this equation is $b_1 \equiv_4 1$, $2 \nmid z_3$ and $d \equiv_4 0$. This means that $b_1 \equiv_4 1$.

Using the same reasoning as in the proof of Lemma 3.3.7, we can prove that $2 \mid z_1 \iff 2 \mid z_2$, $4 \mid z_1 \iff 4 \mid z_2$ and $2 \mid z_1,z_2 \implies 2 \nmid z_3d$.

If $2 \| z_1,z_2$ Equation (3.1.1a) modulo 16 implies that $b_1b_2 \equiv_4 1$ while Equation (3.1.1b) modulo 4 implies that $b_1b_2 \equiv_4 3$. This case is impossible.

If $4 \mid z_1,z_2$, Equation (3.1.1b) modulo 8 implies that $b_1b_2 \equiv_8 7$. This then implies that Equation (3.1.1a) can only have a solution modulo $2^{v_2(e_2)}$ if $2^{(v_2(e_2)-1)/2} \mid z_1,z_2$ because it would otherwise imply that $b_1 - b_2 \equiv_8 0$ which would contradict the fact that $b_1b_2 \equiv_8 7$. We can also study the 2-valuations of the terms in Equation (3.1.1a) and remark that $2^{(v_2(e_2)+1)/2} \nmid z_1,z_2$. Checking Equation (3.1.1a) modulo $2^{v_2(e_2)+2}$ with this new information implies that $b_1 - b_2 \equiv_8 2$. The only pairs (b_1,b_2) respecting both $b_1b_2 \equiv_8 7$ and $b_1 - b_2 \equiv_8 2$ are $(b_1,b_2) \equiv_8 (1,7)$ and $\equiv_8 (5,3)$. In both cases, $b_1 \equiv_4 1$.

This concludes the case when $2 \nmid b_1$.

If $2 \mid b_1$, using the same reasoning as in the proof of Lemma 3.3.7, $2 \mid z_1,z_2$, $2 \| d$ and $2 \nmid z_3$.

If $4 \nmid z_1,z_2$, Equation (3.1.1a) modulo 32 implies that $\overline{b_1b_2} \equiv_8 1$. Equation (3.1.1b) modulo 32 then implies that $b_1 - 1 \equiv_8 1$. Since $2 \mid b_1$, the previous equation implies that $\overline{b_1} \equiv_4 1$.

If $4 \mid z_1$ or $4 \mid z_2$, the 2-valuations of the terms of Equation (3.1.1a) imply that 4 divides the other one. As in the proof of Lemma 3.3.8, Equation (3.1.1b) modulo 32 then implies that $\overline{b_1b_2} \equiv_8 7$. This then implies that Equation (3.1.1a) can only have a solution modulo $2^{v_2(e_2)+2}$ if $2^{(v_2(e_2)+1)/2} \mid z_1,z_2$. Studying Equation (3.1.1a) modulo $2^{v_2(e_2)+4}$ then implies that $\overline{b_1}z_1'^2 - \overline{b_2}z_2'^2 \equiv_4 \overline{e_2} \equiv_4 1$ with $z_i' = \frac{z_i}{2^{(v_2(e_2)+1)/2}}$. The only solutions are ($2 \mid z_1'$ and $\overline{b_2} \equiv_4 3$) and ($2 \mid z_2'$ and $\overline{b_1} \equiv_4 1$). In both cases $\overline{b_1b_2} \equiv_8 7$ implies that $\overline{b_1} \equiv_4 1$.

This concludes the case when $2 \mid b_1$. □

Lemma 3.3.11. *If $\overline{e_2} \equiv_4 1$, $\overline{e_3} \equiv_8 5$ and Equation System (3.1.1) has a non trivial solution in $\mathbb{Q}_2$, then:*

$$\begin{cases} 2 \nmid b_1 \implies \overline{b_2} \equiv_4 1, \\ 2 \mid b_1 \implies \overline{b_2} \equiv_4 3. \end{cases}$$

Proof. The proof of this lemma is practically identical to the proof of Lemma 3.3.10 with two differences.

We study Equation (3.1.1c) instead of Equation (3.1.1b). This gives a condition on b_2 instead of b_1.

Because $\overline{e_3} \equiv_8 5$ instead of $\overline{e_3} \equiv_8 1$, this changes the value of $\overline{b_2}$ when $2 \mid b_1$ for Equation (3.1.1c) to have a solution. □

Lemma 3.3.12. *If $\overline{e_2} \equiv_4 3$, $\overline{e_3} \equiv_8 1$ and Equation System (3.1.1) has a non trivial solution in $\mathbb{Q}_2$, then:*

$$\overline{b_2} \equiv_4 1.$$

PROOF. The proof of this lemma is practically identical to the proof of Lemma 3.3.10 with one difference.

We study Equation (3.1.1c) instead of Equation (3.1.1b). This gives a condition on b_2 instead of b_1. □

Lemma 3.3.13. *If $\overline{e_2} \equiv_4 3$, $\overline{e_3} \equiv_8 5$ and Equation System (3.1.1) has a non trivial solution in $\mathbb{Q}_2$, then:*

$$\begin{cases} 2 \nmid b_1 \implies \overline{b_1} \equiv_4 1, \\ 2 \mid b_1 \implies \overline{b_1} \equiv_4 3. \end{cases}$$

PROOF. The proof of this lemma is practically identical to the proof of Lemma 3.3.10 with one difference.

Because $\overline{e_3} \equiv_8 5$ instead of $\overline{e_3} \equiv_8 1$, this changes the value of $\overline{b_1}$ when $2 \mid b_1$ for Equation (3.1.1b) to have a solution. □

The combination of the above lemmas forms our conditions in the case where $32 \mid e_2$, $v_2(e_2) \equiv_2 1$ and $2 \nmid e_3$.

3.3.2.2. Proofs when $32 \mid e_2$, $v_2(e_2) \equiv_2 0$ and $2 \nmid e_3$:

Lemma 3.3.14. *If Equation System (3.1.1) has a non trivial solution in $\mathbb{Q}_2$, then:*

$$2 \mid b_1 \iff 2 \mid b_2.$$

PROOF. Since this condition only depends on the fact that $2 \mid e_2$ and $2 \nmid e_3$, the proof of this lemma is exactly the same as the proof of Lemma 3.3.6. □

Lemma 3.3.15. *If $\overline{e_3} \equiv_8 3$ and Equation System (3.1.1) has a non trivial solution in $\mathbb{Q}_2$, then:*

$$2 \nmid b_1.$$

Proof. This proof will be done by contradiction. If $2 \mid b_1$, Lemma 3.3.14 implies that $2 \mid b_2$. The 2-valuations of the terms of Equation (3.1.1b) imply that $2 \mid z_1$ and that $2 \mid d$. In the same way, Equation (3.1.1c) implies that $2 \mid z_2$. Since $GCD(z_1,z_2,z_3,d) = 1$, $2 \nmid z_3$. The 2-valuations of the terms of Equation (3.1.1b) then imply that $4 \nmid d$.

Equation (3.1.1b) modulo 32 becomes $b_1 z_1'^2 - \overline{b_1 b_2} \equiv_8 3$ when divided by 4 (with $z_1' = \frac{z_1}{2}$). In order for Equation (3.1.1b) to have a solution modulo 32, either ($4 \mid z_1$ and $\overline{b_1} \equiv_8 5\overline{b_2}$) or ($4 \nmid z_1$ and $b_1 - \overline{b_1 b_2} \equiv_8 3$).

If $4 \mid z_1$ and $\overline{b_1} \equiv_8 5\overline{b_2}$, the fact that $\overline{b_1} \not\equiv_8 \overline{b_2}$ implies that $2^{(v_2(e_2))/2} \mid\mid z_1,z_2$ in order for Equation (3.1.1a) to have a solution modulo $2^{v_2(e_2)+2}$. Equation (3.1.1a) modulo $2^{v_2(e_2)+3}$ then becomes $\overline{b_1 z_1^2} - \overline{b_2 z_2^2} \equiv_{16} 6$ and has no solution with $\overline{b_1} \equiv_8 5\overline{b_2}$. This case is then impossible.

If $4 \nmid z_1$ and $b_1 - \overline{b_1 b_2} \equiv_8 3$, the 2-valuations of the terms of Equation (3.1.1a) imply that $4 \nmid z_2$ because $4 \nmid z_1$. Equation (3.1.1a) then implies that $\overline{b_1 b_2} \equiv_8 1$. This then means that $b_1 - 1 \equiv_8 3$ and that $b_1 \equiv_8 4$. This is impossible since $4 \nmid b_1$.

Since none of the cases are possible, we conclude that $2 \nmid b_1$. □

Lemma 3.3.16. *If $\overline{e_3} \equiv_8 3$ and Equation System (3.1.1) has a non trivial solution in $\mathbb{Q}_2$, then:*

$$\overline{b_1 b_2} \equiv_4 1.$$

Proof. Lemmas 3.3.14 and 3.3.15 imply that $2 \nmid b_1 b_2$.

If 2 divides z_1 or z_2, Equation (3.1.1a) implies that 2 divides the other one. Equation (3.1.1b) then implies that $2 \nmid z_3 d$ because $GCD(z_1,z_2,z_3,d) = 1$. Equation (3.1.1b) modulo 4 then implies that $b_1 b_2 \equiv_4 1$.

If $2 \nmid z_1 z_2$, Equation (3.1.1a) modulo 4 implies that $b_1 b_2 \equiv_4 1$. □

Lemma 3.3.17. *If $\overline{e_3} \equiv_8 7$ and Equation System (3.1.1) has a non trivial solution in $\mathbb{Q}_2$, then:*

$$\overline{b_1 b_2} \equiv_8 1.$$

Proof. The proof of this lemma is very similar to the proof of Lemma 3.3.7. However, there are some small differences caused by the new 2-valuation of e_2. This proof is easier than the original since there is more information about e_3.

As in Lemma 3.3.7, we separate the proof in two cases depending on the parity of b_1 and separate these cases into subcases depending on the 2-valuations of z_1 and z_2.

If $2 \nmid b_1$, using the same reasoning as in the proof of Lemma 3.3.7, we can show that $2 \mid z_1 \iff 2 \mid z_2$ and $4 \mid z_1 \iff 4 \mid z_2$.

If $2 \nmid z_1$,z_2, Equation (3.1.1a) modulo 8 implies that $b_1 b_2 \equiv_8 1$.

If $2 \mid\mid z_1$,z_2, Equation (3.1.1a) modulo 32 implies that $b_1 b_2 \equiv_8 1$.

If $4 \mid z_1$,z_2, Equation (3.1.1b) implies that $2 \nmid z_3 d$. Equation (3.1.1b) modulo 8 then implies that $b_1 b_2 \equiv_8 1$.

This concludes the case when $2 \nmid b_1$.

If $2 \mid b_1$, Equation (3.1.1b) implies that $2 \mid d$ and then that $2 \mid z_1$. Equation (3.1.1c) then implies that $2 \mid z_2$ and then that $2 \nmid z_3$. Reevaluating the 2-valuations in Equation (3.1.1b) shows that $4 \nmid d$.

If $4 \nmid z_1$,z_2, Equation (3.1.1a) modulo 32 implies that $\overline{b_1 b_2} \equiv_8 1$.

If $4 \mid z_1$ or $4 \mid z_2$, Equation (3.1.1b) or (3.1.1c) respectively implies that $\overline{b_1 b_2} \equiv_8 1$.

This concludes the case when $2 \mid b_1$. □

Lemma 3.3.18. *If $\overline{e_3} \equiv_8 1$ and Equation System (3.1.1) has a non trivial solution in $\mathbb{Q}_2$, then:*

$$\overline{b_1 b_2} \equiv_8 1 \textit{ or } 7.$$

Proof. The proof of this lemma is exactly the same as as the proof of Lemma 3.3.8. □

Lemma 3.3.19. *If $\overline{e_3} \equiv_8 5$ and Equation System (3.1.1) has a non trivial solution in $\mathbb{Q}_2$, then:*

$$\overline{b_1 b_2} \equiv_8 1 \textit{ or } 3.$$

Proof. The proof of this lemma is exactly the same as as the proof of Lemma 3.3.9. □

Lemma 3.3.20. *If $\overline{e_2} \equiv_4 1$, $\overline{e_3} \equiv_8 1$ and Equation System (3.1.1) has a non trivial solution in $\mathbb{Q}_2$, then:*

$$\overline{b_1} \equiv_4 1.$$

Proof. This lemma is very similar to Lemma 3.3.10. The proofs of the two lemmas are also almost the same.

As in Lemma 3.3.10, we separate the proof in two cases depending on the parity of b_1 and separate these cases in subcases depending on the 2-valuations of z_1 and z_2.

If $2 \nmid b_1$, Equation (3.1.1a) implies that $2^i \mid z_1 \iff 2^i \mid z_2$ for $i \leq \frac{v_2(e_2)}{2}$. Equation (3.1.1b) then implies that $2 \mid z_1 \implies 2 \nmid z_3 d$.

If $2 \nmid z_1 z_2$, Equation (3.1.1a) implies that $b_1 \equiv_8 b_2$. Equation (3.1.1b) then becomes $b_1 - z_3^2 \equiv_8 d^2$ and this implies that $b_1 \equiv_4 1$.

If $2 \mid z_1, z_2$ but $2^{v_2(e_2)/2} \nmid z_1, z_2$, Equation (3.1.1b) implies that $b_1 b_2 \equiv_4 3$ while Equation (3.1.1a) implies that $b_1 b_2 \equiv_4 1$. This case is impossible.

If $2^{v_2(e_2)/2} \mid z_1, z_2$, Equation (3.1.1a) modulo $2^{v_2(e_2)+2}$ is $b_1 z_1'^2 - b_2 z_2^2 \equiv_4 \overline{e_2} \equiv_4 1$ with $z_i' = \frac{z_i}{2^{v_2(e_2)/2}}$. In order for Equation (3.1.1a) to have a solution, either ($b_1 \equiv_4 1$ and $2 \mid z_2'$) or ($b_2 \equiv_4 3$ and $2 \mid z_1'$). Since Equation (3.1.1b) implies that $b_1 b_2 \equiv_8 7$. We have that $b_1 \equiv_4 1$ in both cases.

This concludes the case when $2 \nmid b_1$.

If $2 \mid b_1$, Equation (3.1.1b) implies that $2 \mid d$ and $2 \mid z_1$. Equation (3.1.1c) implies that $2 \mid z_2$ and $2 \nmid z_3$. Equation (3.1.1b) then implies that $4 \nmid d$. Equation (3.1.1a) also implies that $4 \mid z_1 \iff 4 \mid z_2$.

If $2 \mid\mid z_1$,z_2, Equation (3.1.1a) implies that $\overline{b_1 b_2} \equiv_8 1$. Equation (3.1.1b) modulo 32 implies that $b_1 - 1 \equiv_8 1$ which in turn implies that $\overline{b_1} \equiv_4 1$.

If $4 \mid z_1$,z_2 and $2^{v_2(e_2)/2-1} \nmid z_1$,$z_2$, Equation (3.1.1a) implies that $\overline{b_1 b_2} \equiv_8 1$. However, Equation (3.1.1b) modulo 32 then implies that $0 - 1 \equiv_8 e_3 \equiv_8 1$ which is a contradiction. This case is impossible.

If $2^{v_2(e_2)/2-1} \mid z_1$ or $2^{v_2(e_2)/2-1} \mid z_2$, Equation (3.1.1a) implies that $2^{v_2(e_2)/2-1}$ divides the other one. Equation (3.1.1b) implies that $\overline{b_1 b_2} \equiv_8 7$. The 2-valuations of the terms of Equation (3.1.1a) then imply that $2^{v_2(e_2)/2-1} \mid\mid z_1, z_2$. We can divide Equation (3.1.1a) by $2^{v_2(e_2)+1}$ to get that $\overline{b_1} - \overline{b_2} \equiv_8 2$. When combined with the fact that $\overline{b_1 b_2} \equiv_8 7$, this implies that $\overline{b_1} \equiv_4 1$.

This concludes the case when $2 \mid b_1$. □

Lemma 3.3.21. *If $\overline{e_2} \equiv_4 1$, $\overline{e_3} \equiv_8 5$ and Equation System (3.1.1) has a non trivial solution in $\mathbb{Q}_2$, then:*

$$\begin{cases} 2 \nmid b_1 \implies \overline{b_1} \equiv_4 1, \\ 2 \mid b_1 \implies \overline{b_1} \equiv_4 3. \end{cases}$$

Proof. The proof of this lemma is practically identical to the proof of Lemma 3.3.20 with one difference.

Because $\overline{e_3} \equiv_8 5$ instead of $\overline{e_3} \equiv_8 1$, this changes the value of $\overline{b_1}$ when $2 \mid b_1$ for Equation (3.1.1b) to have a solution. □

Lemma 3.3.22. *If $\overline{e_2} \equiv_4 3$, $\overline{e_3} \equiv_8 1$ and Equation System (3.1.1) has a non trivial solution in $\mathbb{Q}_2$, then:*

$$\overline{b_2} \equiv_4 1.$$

Proof. The proof of this lemma is practically identical to the proof of Lemma 3.3.20 with one difference.

We study Equation (3.1.1c) instead of Equation (3.1.1b). This gives a condition on b_2 instead of b_1. □

Lemma 3.3.23. *If $\overline{e_2} \equiv_4 3$, $\overline{e_3} \equiv_8 5$ and Equation System (3.1.1) has a non trivial solution in $\mathbb{Q}_2$, then:*

$$\begin{cases} 2 \nmid b_1 \implies \overline{b_2} \equiv_4 1, \\ 2 \mid b_1 \implies \overline{b_2} \equiv_4 3. \end{cases}$$

Proof. The proof of this lemma is practically identical to the proof of Lemma 3.3.20 with two differences.

We study Equation (3.1.1c) instead of Equation (3.1.1b). This gives a condition on b_2 instead of b_1.

Because $\overline{e_3} \equiv_8 5$ instead of $\overline{e_3} \equiv_8 1$, this changes the value of $\overline{b_2}$ when $2 \mid b_1$ for Equation (3.1.1c) to have a solution. □

The combination of the above lemmas forms our conditions in the case where $32 \mid e_2$, $v_2(e_2) \equiv_2 0$ and $2 \nmid e_3$.

3.3.2.3. Proofs when $16 \mid e_2$, $v_2(e_2) \equiv_2 0$ and $2 \mid e_3$: When $2 \mid e_3$, the conditions can be separated in three. One condition on $\overline{b_1}$, one on $\overline{b_2}$ and one on $\overline{b_1 b_2}$. These conditions depend on the parity of b_1 and b_2.

Lemma 3.3.24. *The necessary conditions on $\overline{b_1 b_2}$ for Equation System (3.1.1) to have a non-trivial solution in $\mathbb{Q}_2$ are:*

$$\begin{cases} 2 \nmid b_1, 2 \nmid b_2 \implies \overline{b_1 b_2} \equiv_4 1, \\ 2 \nmid b_1, 2 \mid b_2 \implies -\overline{b_1 b_2}\overline{e_3} \equiv_4 1, \\ 2 \mid b_1, 2 \nmid b_2 \implies -\overline{b_1 b_2}\overline{e_3} \equiv_4 1, \\ 2 \mid b_1, 2 \mid b_2 \implies \overline{b_1 b_2} \equiv_4 1. \end{cases}$$

Proof. If $2 \nmid b_1$ and $2 \nmid b_2$:

If $2 \nmid z_1,z_2$, Equation (3.1.1a) implies that $b_1 b_2 \equiv_4 1$.

If $2 \mid z_1,z_2$, the 2-valuations of the terms in Equation (3.1.1b) imply that $2 \mid z_3,d$. This case is impossible since $GCD(z_1,z_2,z_3,d) = 1$.

If $2 \nmid b_1$ and $2 \mid b_2$:

The 2-valuations of the terms in Equation (3.1.1a) imply that $2 \mid z_2$ and $4 \mid z_1$. Equation (3.1.1b) then implies that $2 \nmid z_3 d$ and then that $-\overline{b_1 b_2}\overline{e_3} \equiv_4 1$.

If $2 \mid b_1$ and $2 \nmid b_2$:

Equation (3.1.1a) implies that $2 \mid z_1$ and $4 \mid z_2$. Equation (3.1.1c) then implies that $2 \nmid z_3d$ and then that $-\overline{b_1b_2}\overline{e_3} \equiv_4 1$.

If $2 \mid b_1$ and $2 \mid b_2$:

If $2 \nmid z_1$,z_2, Equation (3.1.1a) implies that $b_1b_2 \equiv_4 1$.

If $2 \mid z_1$,z_2, Equation (3.1.1b) implies that $2 \mid z_3$,d. This case is impossible. □

Lemma 3.3.25. *If $\overline{e_3} \equiv_4 1$, the necessary conditions on $\overline{b_1}$ for Equation System (3.1.1) to have a non-trivial solution in $\mathbb{Q}_2$ are:*

$$\begin{cases} 2 \nmid b_1, 2 \nmid b_2 \implies \overline{b_1} \equiv_8 1 \ \mathit{or}\ 3, \\ 2 \nmid b_1, 2 \mid b_2 \implies \overline{b_1}\overline{e_2} \equiv_8 1 \ \mathit{or}\ 3, \\ 2 \mid b_1, 2 \nmid b_2 \implies \overline{b_1}\overline{e_2}\overline{e_3} \equiv_8 1 \ \mathit{or}\ 3, \\ 2 \mid b_1, 2 \mid b_2 \implies \overline{b_1}\overline{e_3} \equiv_8 1 \ \mathit{or}\ 3. \end{cases}$$

Proof. If $2 \nmid b_1$ and $2 \nmid b_2$:

If $2 \nmid z_1$,z_2, Equation (3.1.1a) implies that $b_1b_2 \equiv_8 1$. Equation (3.1.1b) then implies that $2 \nmid z_3$. Equation (3.1.1b) then implies that $b_1 - 1 \equiv_8 2d^2$. This implies that $\overline{b_1} \equiv_8 1$ or 3.

If $2 \mid z_1$,z_2, Equation (3.1.1b) implies that $2 \mid z_3$,d. This case is impossible.

If $2 \nmid b_1$ and $2 \mid b_2$:

Equation (3.1.1a) implies that $2 \mid z_1$ and $2 \mid z_2$. Equation (3.1.1b) then implies that $2 \nmid z_3d$. Equation (3.1.1a) then implies that $2^{v_2(e_2)/2} \mid\mid z_1$ and $2^{v_2(e_2)/2} \mid z_2$. Equation (3.1.1a) then implies that $b_1 - b_2z_2'^2 \equiv_8 \overline{e_2}$ with $z_2' = \frac{z_2}{2^{v_2(e_2)/2}}$.

If $2 \nmid z_2'$, we can multiply Equation (3.1.1a) by $b_1\overline{e_3}$ to get that $\overline{e_3} - b_1b_2\overline{e_3} \equiv_8 b_1\overline{e_2}\overline{e_3}$. We know from Lemma 3.3.24 that $-\overline{b_1b_2}\overline{e_3} \equiv_4 1$. This implies that $\overline{e_3} + 2 \equiv_8 b_1\overline{e_2}\overline{e_3}$. Since $\overline{e_3} \equiv_4 1$, $b_1\overline{e_2} \equiv_8 3$ for both possible values of $\overline{e_3}$ modulo 8.

If $2 \mid z_2'$, Equation (3.1.1a) implies that $b_1\overline{e_2} \equiv_8 1$.

If $2 \mid b_1$ and $2 \nmid b_2$:

Equation (3.1.1a) implies that $2 \mid z_1$ and $2 \mid z_2$. Equation (3.1.1b) then implies that $2 \nmid z_3d$. Equation (3.1.1a) then implies that $2^{v_2(e_2)/2} \mid z_1$ and $2^{v_2(e_2)/2} \mid\mid z_2$. Equation (3.1.1a) then implies that $b_1z_1'^2 - b_2 \equiv_8 \overline{e_2}$ with $z_1' = \frac{z_1}{2^{v_2(e_2)/2}}$.

If $2 \nmid z_1'$, we can multiply Equation (3.1.1a) by $b_2\overline{e_3}$ to get that $b_1b_2\overline{e_3} - \overline{e_3} \equiv_8 b_2\overline{e_2}\overline{e_3}$. We know from Lemma 3.3.24 that $-\overline{b_1b_2}\overline{e_3} \equiv_4 1$. This implies that $6 - \overline{e_3} \equiv_8$

$b_2\overline{e_2e_3}$. Since $\overline{e_3} \equiv_4 1$, we have that $b_2\overline{e_2} \equiv_8 5$ for both possible values of $\overline{e_3}$ modulo 8. Equation (3.1.1b) also implies that $-\overline{b_1b_2e_3} \equiv_8 1$. Combining the two preceding results implies that $\overline{b_1e_2e_3} \equiv_8 3$

If $2 \mid z_1'$, Equation (3.1.1a) implies that $b_2 \equiv_8 -\overline{e_2}$. Since Equation (3.1.1b) implies that $-\overline{b_1b_2} \equiv_8 \overline{e_3}$, this means that $\overline{b_1}\overline{e_2} \equiv_8 \overline{e_3}$ and then that $\overline{b_1}\overline{e_2e_3} \equiv_8 1$.

If $2 \mid b_1$ and $2 \mid b_2$:

If $2 \nmid z_1$,z_2, Equation (3.1.1a) implies that $b_1b_2 \equiv_8 1$. Equation (3.1.1b) then implies that $2 \nmid d$. It then implies that $\overline{b_1} - 2z_3^2 \equiv_8 \overline{e_3}$. This implies that $\overline{b_1e_3} \equiv_8 1$ or 3 depending on the parity of z_3.

If $2 \mid z_1$,z_2, the 2-valuations of the terms in Equation (3.1.1b) imply that $2 \mid z_3$,d. This case is impossible.

□

Lemma 3.3.26. *If $\overline{e_3} \equiv_4 3$, the necessary conditions on $\overline{b_1}$ for Equation System (3.1.1) to have a non-trivial solution in $\mathbb{Q}_2$ are:*

$$\begin{cases} 2 \nmid b_1, 2 \nmid b_2 \implies \overline{b_1} \equiv_8 1 \textit{ or } 7, \\ 2 \nmid b_1, 2 \mid b_2 \implies \overline{b_1}\overline{e_2} \equiv_8 1 \textit{ or } 7, \\ 2 \mid b_1, 2 \nmid b_2 \implies \overline{b_1}\overline{e_2e_3} \equiv_8 1 \textit{ or } 7, \\ 2 \mid b_1, 2 \mid b_2 \implies \overline{b_1}\overline{e_3} \equiv_8 1 \textit{ or } 7. \end{cases}$$

Proof. The proof of this lemma is almost identical to the proof of Lemma 3.3.25. The only difference is that the change of value of $\overline{e_3}$ modulo 4 causes the right-hand side of each condition to be congruent to 7 instead of 3 modulo 8. □

Lemma 3.3.27. *If $\overline{e_3} \equiv_4 1$, the necessary conditions on $\overline{b_2}$ for Equation System (3.1.1) to have a non-trivial solution in $\mathbb{Q}_2$ are:*

$$\begin{cases} 2 \nmid b_1, 2 \nmid b_2 \implies \overline{b_2} \equiv_8 1 \textit{ or } 3, \\ 2 \nmid b_1, 2 \mid b_2 \implies -\overline{b_2}\overline{e_2e_3} \equiv_8 1 \textit{ or } 3, \\ 2 \mid b_1, 2 \nmid b_2 \implies -\overline{b_2}\overline{e_2} \equiv_8 1 \textit{ or } 3, \\ 2 \mid b_1, 2 \mid b_2 \implies \overline{b_2}\overline{e_3} \equiv_8 1 \textit{ or } 3. \end{cases}$$

Proof. The proof of this lemma is almost the same than the proof of Lemma 3.3.25. The differences being that we study b_2 instead of b_1 and that we check Equation (3.1.1c) instead of Equation (3.1.1b). □

Lemma 3.3.28. *If $\overline{e_3} \equiv_4 3$, the necessary conditions on $\overline{b_2}$ for Equation System (3.1.1) to have a non-trivial solution in $\mathbb{Q}_2$ are:*

$$\begin{cases} 2 \nmid b_1, 2 \nmid b_2 \implies \overline{b_2} \equiv_8 1 \text{ or } 7, \\ 2 \nmid b_1, 2 \mid b_2 \implies \overline{b_2}\overline{e_2}\overline{e_3} \equiv_8 1 \text{ or } 7, \\ 2 \mid b_1, 2 \nmid b_2 \implies \overline{b_2}\overline{e_2} \equiv_8 1 \text{ or } 7, \\ 2 \mid b_1, 2 \mid b_2 \implies \overline{b_2}\overline{e_3} \equiv_8 1 \text{ or } 7. \end{cases}$$

Proof. The proof of this lemma is almost the same than the proof of Lemma 3.3.25. The differences being that we study b_2 instead of b_1 and that we check Equation (3.1.1c) instead of Equation (3.1.1b). □

The combination of the above lemmas forms our conditions in the case where $16 \mid e_2$, $v_2(e_2) \equiv_2 0$ and $2 \mid e_3$.

3.3.2.4. Proofs when $16 \mid e_2$, $v_2(e_2) \equiv_2 1$ and $2 \mid e_3$:

Lemma 3.3.29. *The necessary conditions on $\overline{b_1 b_2}$ for Equation System (3.1.1) to have a non-trivial solution in $\mathbb{Q}_2$ are:*

$$\begin{cases} 2 \nmid b_1, 2 \nmid b_2 \implies \overline{b_1 b_2} \equiv_4 1, \\ 2 \nmid b_1, 2 \mid b_2 \implies -\overline{b_1 b_2}\overline{e_3} \equiv_4 1, \\ 2 \mid b_1, 2 \nmid b_2 \implies -\overline{b_1 b_2}\overline{e_3} \equiv_4 1, \\ 2 \mid b_1, 2 \mid b_2 \implies \overline{b_1 b_2} \equiv_4 1. \end{cases}$$

Proof. The proof of this lemma is exactly the same as the proof to Lemma 3.3.24. □

Lemma 3.3.30. *If $\overline{e_3} \equiv_4 1$, the necessary conditions on $\overline{b_1}$ for Equation System (3.1.1) to have a non-trivial solution in $\mathbb{Q}_2$ are:*

$$\begin{cases} 2 \nmid b_1, 2 \nmid b_2 & \Longrightarrow \overline{b_1} \equiv_8 1 \textit{ or } 3, \\ 2 \nmid b_1, 2 \mid b_2 & \Longrightarrow \overline{b_1}\overline{e_2}\overline{e_3} \equiv_8 1 \textit{ or } 3, \\ 2 \mid b_1, 2 \nmid b_2 & \Longrightarrow \overline{b_1}\overline{e_2} \equiv_8 1 \textit{ or } 3, \\ 2 \mid b_1, 2 \mid b_2 & \Longrightarrow \overline{b_1}\overline{e_3} \equiv_8 1 \textit{ or } 3. \end{cases}$$

Proof. The proof of this lemma is very similar to the proof of Lemma 3.3.25.

The difference is the change of parity of the 2-valuation of e_2. This causes the case when $2 \mid b_1$ and $2 \nmid b_2$ in this lemma to be solved in the same way than the case when $2 \nmid b_1$ and $2 \mid b_2$ in Lemma 3.3.25 and vice versa. □

Lemma 3.3.31. *If $\overline{e_3} \equiv_4 3$, the necessary conditions on $\overline{b_1}$ for Equation System (3.1.1) to have a non-trivial solution in $\mathbb{Q}_2$ are:*

$$\begin{cases} 2 \nmid b_1, 2 \nmid b_2 & \Longrightarrow \overline{b_1} \equiv_8 1 \textit{ or } 7, \\ 2 \nmid b_1, 2 \mid b_2 & \Longrightarrow \overline{b_1}\overline{e_2}\overline{e_3} \equiv_8 1 \textit{ or } 7, \\ 2 \mid b_1, 2 \nmid b_2 & \Longrightarrow \overline{b_1}\overline{e_2} \equiv_8 1 \textit{ or } 7, \\ 2 \mid b_1, 2 \mid b_2 & \Longrightarrow \overline{b_1}\overline{e_3} \equiv_8 1 \textit{ or } 7. \end{cases}$$

Proof. The proof of this lemma is almost identical to the proof of Lemma 3.3.30. The only difference being that the change of value of $\overline{e_3}$ modulo 4 causes the right-hand side of each condition to be congruent to 7 instead of 3 modulo 8. □

Lemma 3.3.32. *If $\overline{e_3} \equiv_4 1$, the necessary conditions on $\overline{b_2}$ for Equation System (3.1.1) to have a non-trivial solution in $\mathbb{Q}_2$ are:*

$$\begin{cases} 2 \nmid b_1, 2 \nmid b_2 & \Longrightarrow \overline{b_2} \equiv_8 1 \textit{ or } 3, \\ 2 \nmid b_1, 2 \mid b_2 & \Longrightarrow -\overline{b_2}\overline{e_2} \equiv_8 1 \textit{ or } 3, \\ 2 \mid b_1, 2 \nmid b_2 & \Longrightarrow -\overline{b_2}\overline{e_2}\overline{e_3} \equiv_8 1 \textit{ or } 3, \\ 2 \mid b_1, 2 \mid b_2 & \Longrightarrow \overline{b_2}\overline{e_3} \equiv_8 1 \textit{ or } 3. \end{cases}$$

Proof. The proof of this lemma is almost the same as the proof of Lemma 3.3.30. The differences being that we study b_2 instead of b_1 and that we check Equation (3.1.1c) instead of Equation (3.1.1b). □

Lemma 3.3.33. *If $\overline{e_3} \equiv_4 3$, the necessary conditions on $\overline{b_2}$ for Equation System (3.1.1) to have a non-trivial solution in $\mathbb{Q}_2$ are:*

$$\begin{cases} 2 \nmid b_1, 2 \nmid b_2 \implies \overline{b_2} \equiv_8 1 \text{ or } 7, \\ 2 \nmid b_1, 2 \mid b_2 \implies \overline{b_2}\overline{e_2} \equiv_8 1 \text{ or } 7, \\ 2 \mid b_1, 2 \nmid b_2 \implies \overline{b_2}\overline{e_2 e_3} \equiv_8 1 \text{ or } 7, \\ 2 \mid b_1, 2 \mid b_2 \implies \overline{b_2}\overline{e_3} \equiv_8 1 \text{ or } 7. \end{cases}$$

Proof. The proof of this lemma is almost the same as the proof of Lemma 3.3.30. The differences being that we study b_2 instead of b_1 and that we check Equation (3.1.1c) instead of Equation (3.1.1b). □

The combination of the above lemmas forms our conditions in the case where $16 \mid e_2$, $v_2(e_2) \equiv_2 1$ and $2 \mid e_3$.

3.3.3. The proofs of sufficiency

As previously stated in Subsection 3.3.2, the proofs for the sufficient conditions are not as relevant for this thesis. The proofs of sufficiency for each case of valuations of (e_2,e_3) are very similar to each other and also rather long. For the sake of brevity, we will start by describing the general idea of the proofs and then explicitly show the proof for one of the cases.

The idea behind the proofs of sufficiency is then to follow a similar method to the proof of Hensel's Lemma for each case.

In order to apply such a method, we start by showing that the conditions under consideration are sufficient in $\mathbb{Z}/2^n\mathbb{Z}$ for an n big enough. For small valuations, this can be done by simply checking by brute force. For big valuations, this is done by reducing the problem to a smaller valuation.

Once the fact that the conditions are sufficient for a solution in $\mathbb{Z}/2^n\mathbb{Z}$ is established, we prove the existence of a solution in $\mathbb{Q}_2$ using induction. We suppose that there is a solution in $\mathbb{Z}/2^m\mathbb{Z}$ for $m \geq n$ (sometimes we will have to take multiple solutions based on the properties of (b_1,b_2) and the rest of the proof becomes a case by case proof) and we then show how to construct a solution in $\mathbb{Z}/2^{m+1}\mathbb{Z}$ from the solution in $\mathbb{Z}/2^m\mathbb{Z}$.

Given our solution in $\mathbb{Z}/2^m\mathbb{Z}$, we look at the triplet $(b_1z_1^2,b_2z_2^2,b_1b_2z_3^2)$ and we choose two of the three terms. It is convenient to choose them with the smallest valuation as it will make the needed m for the induction base smaller. Let us call the two chosen terms aw_1^2 and bw_2^2 while we call the other term cw_3^2. We then choose two of the three equations of Equation System (3.1.1) such that the first chosen contains aw_1^2 and cw_3^2 (but not bw_2^2) while the second contains bw_2^2 (and maybe aw_1^2).

Since we have a solution in $\mathbb{Z}/2^m\mathbb{Z}$, when putting every term on the left side, we have that every equation of Equation System (3.1.1) will be congruent to 0 or 2^m in $\mathbb{Z}/2^{m+1}\mathbb{Z}$.

For the first equation, if it is congruent to 0, there is nothing to do and we proceed to the second equation. However, if it is congruent to 2^m, we apply the transformation $w_1 \mapsto w_1 + 2^k$ with k such that $2^{k+1}aw_1$ is congruent to 2^m modulo 2^{m+1} while $a2^{2k}$ is congruent to 0 modulo 2^{m+1}. The first equation becomes congruent to 0 while the second equation is still congruent to either 0 or 2^m. The chosen m at the start must be big enough for such a k to exist.

We then apply the same method to bw_2^2 in the second equation, but with a new value for k. Since bw_2^2 does not appear in the first equation, we have that, after applying the above transformations, both equations are congruent to 0 in $\mathbb{Z}/2^{m+1}\mathbb{Z}$. We have now a solution in $\mathbb{Z}/2^{m+1}\mathbb{Z}$ and that completes our proof of sufficiency.

To make this clearer, here is the explicit version of one of the proofs:

Proof when $v_2(e_2) = 1$ and $2 \nmid e_3$: We can verify by brute force that the conditions of Theorem 3.3.1 are sufficient for a solution in $\mathbb{Z}/64\mathbb{Z}$. Since we cannot apply Hensel's lemma, we proceed by induction.

Let the pair (b_1,b_2) respect the given conditions. Suppose that those conditions are sufficient for a solution in $\mathbb{Z}/2^m\mathbb{Z}$ with $m \geq 6$, we will show that there is a solution in $\mathbb{Z}/2^{m+1}\mathbb{Z}$.

Before starting the induction, we need to state some facts. We shall separate the problem in two cases based on the 2-valuations of b_1 and b_2.

Case 1. If $2 \nmid b_1,b_2$, Equation (3.1.1a) implies that $2 \mid z_1 \iff 2 \mid z_2$. However, if $2 \mid z_1,z_2$, Equation (3.1.1a) implies that $2 \mid d$ and then Equation $3.1.1b$ implies that $2 \mid z_3$. Since 2 cannot divide all the variables z_1,z_2,z_3,d, we have that $2 \nmid z_1,z_2$. We can now look at the equation system in $\mathbb{Z}/2^{m+1}\mathbb{Z}$ when the variables give a solution in $\mathbb{Z}/2^m\mathbb{Z}$. Since it suffices to satisfy two of the three equations, we will look at the second and third equations:

$$\begin{cases} b_1z_1^2 - b_1b_2z_3^2 - e_3d^2 \equiv_{2^{m+1}} x_1, \\ b_2z_2^2 - b_1b_2z_3^2 - (e_3 - e_2)d^2 \equiv_{2^{m+1}} x_2, \end{cases}$$

with x_1,$x_2 \in \{0, 2^m\}$. Our goal is to have 0 on the right side of both equations. Let us define $a_1 = e_3$ and $a_2 = e_3 - e_2$. For $i \in \{1,2\}$, if $x_i = 0$ the z_i yield a solution modulo 2^{m+1}. However, if $x_i = 2^m$, we apply the transformation $z_i \mapsto z_i + 2^{m-1}$. We then get the equation:

$$b_i(z_i + 2^{m-1})^2 - b_1b_2z_3^2 - a_id^2 \equiv_{2^{m+1}} x_i + b_iz_i2^m + 2^{2m-2}.$$

Since, $2 \nmid b_iz_i$ and $m \geq 6$, we have that $b_iz_i2^m \equiv_{2^{m+1}} 2^m$ and that $2^{2m-2} \equiv_{2^{m+1}} 0$. Then this gives a solution modulo 2^{m+1}.

Case 2. If $2 \mid b_1$,b_2, Equation (3.1.1b) implies that $2 \mid d$. Equations (3.1.1b) and (3.1.1c) then imply that $2 \mid z_1$ and $2 \mid z_2$ respectively. Since we asked for 2 not to divide all the variables, we have that $2 \nmid z_3$. Equation (3.1.1b) then implies that $4 \nmid d$. This then implies that $4 \nmid z_1$ or $4 \nmid z_2$ in order for Equation (3.1.1a) to have a solution. We can now look at our equation system in $\mathbb{Z}/2^{m+1}\mathbb{Z}$ when our variables give a solution in $\mathbb{Z}/2^m\mathbb{Z}$. Since we only need to verify two of the three equations, we will look at the second and third equations:

$$\begin{cases} b_1z_1^2 - b_1b_2z_3^2 - e_3d^2 \equiv_{2^{m+1}} x_1, \\ b_2z_2^2 - b_1b_2z_3^2 - (e_3 - e_2)d^2 \equiv_{2^{m+1}} x_2, \end{cases}$$

with x_1,$x_2 \in \{0, 2^m\}$. Our goal is to have 0 on the right side of both equations. Since we know that 4 does not divide z_1 or z_2, we will suppose that $4 \nmid z_2$. If this is not the case, we simply flip the order of the equations and change the names of the variables in order to obtain the same proof.

If $x_1 = 0$, there is nothing to do for the first equation. If $x_1 = 2^m$, we apply the transformation $z_3 \mapsto z_3 + 2^{m-3}$. This gives us:

$$\begin{cases} b_1z_1^2 - b_1b_2(z_3 + 2^{m-3})^2 - e_3d^2 \equiv_{2^{m+1}} x_1 - b_1b_2z_32^{m-2} + b_1b_22^{2m-6}, \\ b_2z_2^2 - b_1b_2(z_3 + 2^{m-3})^2 - (e_3 - e_2)d^2 \equiv_{2^{m+1}} x_2 - b_1b_2z_32^{m-2} + b_1b_22^{2m-6}. \end{cases}$$

We remark that $4 \mid\mid b_1b_2$ and that $m \geq 6$. This implies that $b_1b_2z_32^{m-2} \equiv_{2^{m+1}} 2^m$, $b_1b_22^{2m-6} \equiv_{2^{m+1}} 0$ and we have:

$$\begin{cases} b_1z_1^2 - b_1b_2(z_3 + 2^{m-3})^2 - e_3d^2 \equiv_{2^{m+1}} x_1 + 2^m \equiv_{2^{m+1}} 0, \\ b_2z_2^2 - b_1b_2(z_3 + 2^{m-3})^2 - (e_3 - e_2)d^2 \equiv_{2^{m+1}} x_2 + 2^m. \end{cases}$$

The rest of the work is similar to the preceding step. Let us denote by y_2 either x_2 or $x_2 + 2^m$ depending on whether we did the transformation or not. Analogously, we denote by w_3 either z_3 or $z_3 + 2^{m-3}$. We have that $y_2 \in \{0,2^m\}$ as before. If $y_2 = 0$, there is nothing to do for the second equation. If $y_2 = 2^m$, we apply the transformation $z_2 \mapsto z_2 + 2^{m-3}$. This gives us:

$$\begin{cases} b_1z_1^2 - b_1b_2w_3^2 - e_3d^2 \equiv_{2^{m+1}} 0, \\ b_2(z_2 + 2^{m-3})^2 - b_1b_2w_3^2 - (e_3 - e_2)d^2 \equiv_{2^{m+1}} y_2 + b_2z_22^{m-2} + b_22^{2m-6}. \end{cases}$$

We remark that $2 \mid\mid b_2$, $2 \mid\mid z_2$ and $m \geq 6$. This implies that $b_2z_22^{m-2} \equiv_{2^{m+1}} 2^m$, $b_22^{2m-6} \equiv_{2^{m+1}} 0$ and we have:

$$\begin{cases} b_1z_1^2 - b_1b_2w_3^2 - e_3d^2 \equiv_{2^{m+1}} 0, \\ b_2(z_2 + 2^{m-3})^2 - b_1b_2w_3^2 - (e_3 - e_2)d^2 \equiv_{2^{m+1}} 0. \end{cases}$$

Therefore, we have obtained a solution.

□

3.4. Conditions in $\mathbb{Q}_p$

Let p be a fixed odd prime. We are only interested in p if it divides $16e_2^2e_3^2(e_3-e_2)^2$. With the reductions discussed in Section 3.1, we can separate our primes in two major cases. Either p only divides one element of $\{e_2,e_3,e_3 - e_2\}$ or p divides all of them.

When p divides only one element, we can consider three sub-cases depending on whether the element is e_2, e_3 or $e_3 - e_2$.

When p divides all three, we can consider four sub-cases, depending on the element with the highest valuation in $\mathbb{Q}_p$. The fourth case is when p divides all three elements exactly.

Since all equations in System (3.1.1) are quadratic forms, looking for solutions in $\mathbb{Q}_p$ is equivalent to looking for solutions in $\mathbb{Z}/p^k\mathbb{Z}$ for all k.

Also, for p an odd prime, we will see that the proofs of sufficiency will be considerably simpler than with $\mathbb{Q}_2$ since we can apply Hensel's Lemma this time.

Before starting, we remark that if $GCD(z_1,z_2,z_3,d) > 1$, we can divide the equation system by its common divisor. Because of this, we can assume that $GCD(z_1,z_2,z_3,d) = 1$. When working in $\mathbb{Q}_p$, this condition simply means that not all variables are multiples of p.

For the sake of clarity, we will first give the conditions and then spend the rest of this section to prove them case by case.

3.4.1. The conditions

For an odd prime p, the conditions for a solution in $\mathbb{Q}_p$ are considerably simpler than in the case of $\mathbb{Q}_2$. As explained in Section 3.1, the third reduction shortened the number of cases in $\mathbb{Q}_2$. Because this reduction does not apply for $p \neq 2$, there are more cases in $\mathbb{Q}_p$ even if each case is simpler.

We also remark that, for e_2 and e_3 fixed, there are always two conditions on the pair (b_1,b_2).

Theorem 3.4.1. *Let $\delta = e_2e_3(e_3 - e_2)$. If $p \mid \delta$ but $p \nmid GCD(e_2,e_3,e_3 - e_2)$, the following conditions are necessary and sufficient for Equation System (3.1.1) to have a non-trivial solution in $\mathbb{Q}_p$:*

			If $p \mid e_2$:		*If* $p \mid e_3$:		*If* $p \mid e_3 - e_2$:	
			If $\left(\frac{-e_3}{p}\right) = 1$:	*If* $\left(\frac{-e_3}{p}\right) = -1$:	*If* $\left(\frac{-e_2}{p}\right) = 1$:	*If* $\left(\frac{-e_2}{p}\right) = -1$:	*If* $\left(\frac{e_3}{p}\right) = 1$:	*If* $\left(\frac{e_3}{p}\right) = -1$:
If $v_p(\delta) \equiv_2 1$:	*If* $p \nmid b_1$:	*If* $p \nmid b_2$:	$\left(\frac{\overline{b_1b_2}}{p}\right) = 1$	$\left(\frac{\overline{b_1b_2}}{p}\right) = 1$	$\left(\frac{\overline{b_2}}{p}\right) = 1$	$\left(\frac{\overline{b_2}}{p}\right) = 1$	$\left(\frac{\overline{b_1}}{p}\right) = 1$	$\left(\frac{\overline{b_1}}{p}\right) = 1$
		If $p \mid b_2$:	*No solution.*	*No solution.*	*No solution.*	*No solution.*	$\left(\frac{\overline{b_1}}{p}\right) = 1$	$\left(\frac{\overline{b_1}}{p}\right) = -1$
	If $p \mid b_1$:	*If* $p \nmid b_2$:	*No solution.*	*No solution.*	$\left(\frac{\overline{b_2}}{p}\right) = 1$	$\left(\frac{\overline{b_2}}{p}\right) = -1$	*No solution.*	*No solution.*
		If $p \mid b_2$:	$\left(\frac{\overline{b_1b_2}}{p}\right) = 1$	$\left(\frac{\overline{b_1b_2}}{p}\right) = -1$	*No solution.*	*No solution.*	*No solution.*	*No solution.*
If $v_p(\delta) \equiv_2 0$:	*If* $p \nmid b_1$:	*If* $p \nmid b_2$:	$\left(\frac{\overline{b_1b_2}}{p}\right) = 1$	*No additional condition.*	$\left(\frac{\overline{b_2}}{p}\right) = 1$	*No additional condition.*	$\left(\frac{\overline{b_1}}{p}\right) = 1$	*No additional condition.*
		If $p \mid b_2$:	*No solution.*	*No solution.*	*No solution.*	*No solution.*	$\left(\frac{\overline{b_1}}{p}\right) = 1$	*No solution.*
	If $p \mid b_1$:	*If* $p \nmid b_2$:	*No solution.*	*No solution.*	$\left(\frac{\overline{b_2}}{p}\right) = 1$	*No solution.*	*No solution.*	*No solution.*
		If $p \mid b_2$:	$\left(\frac{\overline{b_1b_2}}{p}\right) = 1$	*No solution.*	*No solution.*	*No solution.*	*No solution.*	*No solution.*

Table 3.5. Conditions for a solution in $\mathbb{Q}_p$ when $p \mid \delta$ but $p \nmid GCD(e_2,e_3,e_3 - e_2)$.

Theorem 3.4.2. *Let $\delta = e_2 e_3 (e_3 - e_2)$. If $p \mid GCD(e_2{,}e_3{,}e_3 - e_2)$, the following conditions are necessary and sufficient for Equation System (3.1.1) to have a non-trivial solution in $\mathbb{Q}_p$:*

			If $p^2 \nmid e_2{,}e_3{,}(e_3 - e_2)$:	*If* $p^2 \mid e_2$:	*If* $p^2 \mid e_3$:	*If* $p^2 \mid (e_3 - e_2)$:
If $v_p(\delta) \equiv_2 0$:	*If* $p \nmid b_1$:	*If* $p \nmid b_2$:	N/A	$\left(\frac{\overline{b_1}}{p}\right) = 1$ $\left(\frac{\overline{b_2}}{p}\right) = 1$	$\left(\frac{\overline{b_1}}{p}\right) = 1$ $\left(\frac{\overline{b_2}}{p}\right) = 1$	$\left(\frac{\overline{b_1}}{p}\right) = 1$ $\left(\frac{\overline{b_2}}{p}\right) = 1$
		If $p \mid b_2$:	N/A	$\left(\frac{\overline{b_1 e_2}}{p}\right) = 1$ $\left(\frac{\overline{-b_2 e_2 e_3}}{p}\right) = 1$	$\left(\frac{\overline{b_1 e_3}}{p}\right) = 1$ $\left(\frac{\overline{-b_2 e_2}}{p}\right) = 1$	$\left(\frac{\overline{b_1}}{p}\right) = 1$ $\left(\frac{\overline{-b_2 e_2}}{p}\right) = 1$
	If $p \mid b_1$:	*If* $p \nmid b_2$:	N/A	$\left(\frac{\overline{b_1 e_2 e_3}}{p}\right) = 1$ $\left(\frac{\overline{-b_2 e_2}}{p}\right) = 1$	$\left(\frac{\overline{b_1 e_2}}{p}\right) = 1$ $\left(\frac{\overline{b_2}}{p}\right) = 1$	$\left(\frac{\overline{b_1 e_2}}{p}\right) = 1$ $\left(\frac{\overline{b_2 (e_3 - e_2)}}{p}\right) = 1$
		If $p \mid b_2$:	N/A	$\left(\frac{\overline{b_1 e_3}}{p}\right) = 1$ $\left(\frac{\overline{b_2 e_3}}{p}\right) = 1$	$\left(\frac{\overline{b_1 e_2 e_3}}{p}\right) = 1$ $\left(\frac{\overline{-b_2 e_2}}{p}\right) = 1$	$\left(\frac{\overline{b_1 e_2}}{p}\right) = 1$ $\left(\frac{\overline{-b_2 e_2 (e_3 - e_2)}}{p}\right) = 1$
If $v_p(\delta) \equiv_2 1$:	*If* $p \nmid b_1$:	*If* $p \nmid b_2$:	$\left(\frac{\overline{b_1}}{p}\right) = 1$ $\left(\frac{\overline{b_2}}{p}\right) = 1$	$\left(\frac{\overline{b_1}}{p}\right) = 1$ $\left(\frac{\overline{b_2}}{p}\right) = 1$	$\left(\frac{\overline{b_1}}{p}\right) = 1$ $\left(\frac{\overline{b_2}}{p}\right) = 1$	$\left(\frac{\overline{b_1}}{p}\right) = 1$ $\left(\frac{\overline{b_2}}{p}\right) = 1$
		If $p \mid b_2$:	$\left(\frac{\overline{b_1 e_2 e_3}}{p}\right) = 1$ $\left(\frac{\overline{-b_2 e_2}}{p}\right) = 1$	$\left(\frac{\overline{b_1 e_2 e_3}}{p}\right) = 1$ $\left(\frac{\overline{-b_2 e_2}}{p}\right) = 1$	$\left(\frac{\overline{b_1 e_2 e_3}}{p}\right) = 1$ $\left(\frac{\overline{-b_2 e_2}}{p}\right) = 1$	$\left(\frac{\overline{b_1}}{p}\right) = 1$ $\left(\frac{\overline{-b_2 e_2}}{p}\right) = 1$
	If $p \mid b_1$:	*If* $p \nmid b_2$:	$\left(\frac{\overline{b_1 e_2}}{p}\right) = 1$ $\left(\frac{\overline{-b_2 e_2 (e_3 - e_2)}}{p}\right) = 1$	$\left(\frac{\overline{b_1 e_2}}{p}\right) = 1$ $\left(\frac{\overline{-b_2 e_2 e_3}}{p}\right) = 1$	$\left(\frac{\overline{b_1 e_2}}{p}\right) = 1$ $\left(\frac{\overline{b_2}}{p}\right) = 1$	$\left(\frac{\overline{b_1 e_2}}{p}\right) = 1$ $\left(\frac{\overline{-b_2 e_2 (e_3 - e_2)}}{p}\right) = 1$
		If $p \mid b_2$:	$\left(\frac{\overline{b_1 e_3}}{p}\right) = 1$ $\left(\frac{\overline{b_2 (e_3 - e_2)}}{p}\right) = 1$	$\left(\frac{\overline{b_1 e_3}}{p}\right) = 1$ $\left(\frac{\overline{b_2 e_3}}{p}\right) = 1$	$\left(\frac{\overline{b_1 e_3}}{p}\right) = 1$ $\left(\frac{\overline{-b_2 e_2}}{p}\right) = 1$	$\left(\frac{\overline{b_1 e_2}}{p}\right) = 1$ $\left(\frac{\overline{b_2 (e_3 - e_2)}}{p}\right) = 1$

Table 3.6. Conditions for a solution in $\mathbb{Q}_p$ when $p \mid GCD(e_2{,}e_3{,}e_3 - e_2)$.

3.4.2. The proofs of necessity

As in the case of the conditions in $\mathbb{Q}_2$, we will separate the proofs of necessity from the proofs of sufficiency. However, since the prime p is undetermined, we cannot use brute force proofs.

We remark that every equation in System (3.1.1) has three terms. We will show in each case that the given conditions are necessary for a non-trivial solution in $\mathbb{Z}/p\mathbb{Z}$. By non trivial, we mean that, if p divides all three terms of an equation, we divide all three terms by p until there is at least one term that is not a multiple of p.

The necessary conditions can be separated in multiple cases organized in four different lemmas.

3.4.2.1. Proofs when $p \mid e_2$ and $p \nmid e_3$:

Lemma 3.4.3. *If Equation System (3.1.1) has a non trivial solution in $\mathbb{Q}_p$, then:*

$$p \mid b_1 \iff p \mid b_2.$$

Proof. This lemma is very similar to Lemma 3.3.6 but we study p-valuations instead of 2-valuations.

This can be done by contradiction. If $p \mid b_1$ and $p \nmid b_2$, Equation (3.1.1b) implies that $p \mid d$, then Equation (3.1.1a) implies that $p \mid z_2$, then Equation (3.1.1c) implies that $p \mid z_3$, then Equation (3.1.1a) implies that $p \mid z_1$ and that is a contradiction.

If $p \nmid b_1$ and $p \mid b_2$, Equation (3.1.1c) implies that $p \mid d$, then Equation (3.1.1a) implies that $p \mid z_1$, then Equation (3.1.1b) implies that $p \mid z_3$, then Equation (3.1.1a) implies that $p \mid z_2$ and that is another contradiction. □

Lemma 3.4.4. *If $v_p(e_2) \equiv_2 0$, $\left(\frac{-e_3}{p}\right) = -1$ and Equation System (3.1.1) has a non trivial solution in $\mathbb{Q}_p$, then:*

$$p \nmid b_1.$$

Proof. If $p \mid b_1$,b_2:

Equation (3.1.1b) implies that $p \mid d$. Equation (3.1.1b) then implies that $p \mid z_1$ and Equation (3.1.1c) then implies that $p \mid z_2$. We then need that $p \nmid z_3$. Equation (3.1.1b) then implies that $p \mid\mid d$ and that $\left(\frac{\overline{-e_3 b_1 b_2}}{p}\right) = -\left(\frac{\overline{b_1 b_2}}{p}\right) = 1$.

However, Equation (3.1.1a) implies that $\left(\frac{\overline{b_1b_2}}{p}\right) = 1$. Contradiction. $\square$

Lemma 3.4.5. *If $v_p(e_2) \equiv_2 1$ or $\left(\frac{-e_3}{p}\right) = 1$. If Equation System (3.1.1) has a non trivial solution in $\mathbb{Q}_p$, then:*

$$\begin{cases} p \nmid b_1 \implies \left(\dfrac{\overline{b_1b_2}}{p}\right) = 1, \\ p \mid b_1 \implies \left(\dfrac{\overline{-e_3b_1b_2}}{p}\right) = 1. \end{cases}$$

Proof. If $p \nmid b_1,b_2$:

If $p \nmid z_1,z_2$, Equation (3.1.1a) implies that $\left(\frac{\overline{b_1b_2}}{p}\right) = 1$.

If $p \mid z_1$ or $p \mid z_2$, Equation (3.1.1a) implies that p divides both.

If $\left(\frac{-e_3}{p}\right) = 1$, Equation (3.1.1b) implies that $\left(\frac{\overline{b_1b_2}}{p}\right) = 1$.

If $v_p(e_2) \equiv_2 1$, the p-valuations of the terms in Equation (3.1.1a) imply that $v_p(z_1) = v_p(z_2)$ and $v_p(e_2d^2) > v_p(b_1z_1^2) = v_p(b_2z_2^2)$. Equation (3.1.1a) then implies that $\left(\frac{\overline{b_1b_2}}{p}\right) = 1$.

If $p \mid b_1,b_2$:

Equation (3.1.1b) implies that $p \mid d,z_1$. Equation (3.1.1c) then implies that $p \mid z_2$ and $p \nmid z_3$. Equation (3.1.1b) then implies that $p \mid\mid d$ and that $\left(\frac{\overline{-e_3b_1b_2}}{p}\right)$. $\square$

The combination of the above lemmas forms our conditions in the case where $p \mid e_2$ and $p \nmid e_3$.

3.4.2.2. Proofs when $p \nmid e_2$ and $p \mid e_3$:

Lemma 3.4.6. *If Equation System (3.1.1) has a non trivial solution in $\mathbb{Q}_p$, then:*

$$p \nmid b_2.$$

Proof. If $p \mid b_1$ and $p \mid b_2$, Equation (3.1.1a) implies that $p \mid d$. Then, Equation (3.1.1b) and Equation (3.1.1c) imply that $p \mid z_1$ and $p \mid z_2$ respectively. Equation (3.1.1b) then implies $p \mid z_3$. Contradiction.

If $p \nmid b_1$ and $p \mid b_2$, Equation (3.1.1c) implies that $p \mid d$. Equation (3.1.1b) then implies that $p \mid z_1$. Equation (3.1.1a) then implies that $p \mid z_2$. Equation (3.1.1b) then implies that $p \mid z_3$. Contradiction. $\square$

Lemma 3.4.7. *If $v_p(e_3) \equiv_2 0$, $\left(\frac{-e_2}{p}\right) = -1$ and Equation System (3.1.1) has a non trivial solution in $\mathbb{Q}_p$, then:*

$$p \nmid b_1.$$

Proof. If $p \mid b_1$:

If $p \mid z_2$ or $p \mid d$, Equation (3.1.1a) implies that p divides the other one. It then follows that $p \mid z_1$ and Equation (3.1.1b) implies that $p \mid z_3$. Contradiction.

If $p \nmid z_2$,d, Equation (3.1.1a) implies that $\left(\frac{b_2}{p}\right) = \left(\frac{-e_2}{p}\right) = -1$. However, Equation (3.1.1b) implies that $\left(\frac{b_2}{p}\right) = 1$. Contradiction. □

Lemma 3.4.8. *If $v_p(e_3) \equiv_2 1$ or $\left(\frac{-e_2}{p}\right) = 1$. If Equation System (3.1.1) has a non trivial solution in $\mathbb{Q}_p$, then:*

$$\begin{cases} p \nmid b_1 \implies \left(\dfrac{b_2}{p}\right) = 1, \\ p \mid b_1 \implies \left(\dfrac{-e_2 b_2}{p}\right) = 1. \end{cases}$$

Proof. If $p \nmid b_1$:

If $p \nmid z_1$,z_3, Equation (3.1.1b) implies that $\left(\frac{b_2}{p}\right) = 1$.

If $p \mid z_1$ or $p \mid z_3$, Equation (3.1.1b) implies that p divides the other one. Equation (3.1.1a) then implies that $p \nmid z_2$,d. If $v_p(e_3) \equiv_2 1$, Equation (3.1.1b) implies that $\left(\frac{b_2}{p}\right) = 1$. If $\left(\frac{-e_2}{p}\right) = 1$, Equation (3.1.1a) implies that $\left(\frac{b_2}{p}\right) = 1$.

If $p \mid b_1$:

If $p \nmid z_2$,d, Equation (3.1.1a) implies that $\left(\frac{-e_2 b_2}{p}\right) = 1$.

If $p \mid z_2$ or $p \mid d$, Equation (3.1.1a) implies that p divides both. Equation (3.1.1c) then implies that $p \nmid z_3$ and then Equation (3.1.1b) implies that $p \mid z_1$. Contradiction. □

The combination of the above lemmas forms our conditions in the case where $p \nmid e_2$ and $p \mid e_3$.

3.4.2.3. Proofs when $p \mid (e_3 - e_2)$ and $p \nmid e_2$: If we exchange Equation (3.1.1b) with Equation (3.1.1c), we remark that we can write the equation system as:

$$\begin{cases} b_2z_2^2 - b_1z_1^2 = (-e_2)d^2, \\ b_2z_2^2 - b_1b_2z_3^2 = (e_3 - e_2)d^2, \\ b_1z_1^2 - b_1b_2z_3^2 = ((e_3 - e_2) - (-e_2))d^2, \end{cases}$$

which is simply a system that respects the conditions of our original system but with $e_2 \mapsto -e_2$, $e_3 \mapsto (e_3 - e_2)$, $b_1 \rightleftarrows b_2$ and $z_1 \rightleftarrows z_2$.

We can then simply use the proofs of the case where $p \nmid e_2$ and $p \mid e_3$.

3.4.2.4. Proofs when $p \mid\mid e_2$, $p \mid\mid e_3$ and $p \mid\mid (e_3 - e_2)$:

Lemma 3.4.9. *If $p \nmid b_1$, $p \nmid b_2$ and Equation System (3.1.1) has a non trivial solution in $\mathbb{Q}_p$, then:*

$$\begin{cases} \left(\dfrac{b_1}{p}\right) = 1, \\ \left(\dfrac{b_2}{p}\right) = 1. \end{cases}$$

Proof. First, we remark that as soon as $p \mid z_i$ for some i, $p \mid z_j$ for all j. So we need $p \nmid z_1z_2z_3$.

The first condition then comes from Equation (3.1.1c).

The second condition then comes from Equation (3.1.1b). □

Lemma 3.4.10. *If $p \mid b_1$, $p \nmid b_2$ and Equation System (3.1.1) has a non trivial solution in $\mathbb{Q}_p$, then:*

$$\begin{cases} \left(\dfrac{\overline{b_1}\overline{e_2}}{p}\right) = 1, \\ \left(\dfrac{-\overline{b_1}b_2\overline{(e_3 - e_2)}}{p}\right) = 1. \end{cases}$$

Proof. In order for Equation (3.1.1a) to have a solution, we need that $p \mid z_2$. If we had that $p \mid d$ or $p \mid z_1$, Equation (3.1.1a) would give us the other one. If we had that $p \mid d$ or $p \mid z_3$, Equation (3.1.1b) would give us the other one. We then get that $p \nmid z_1z_3d$.

We can then divide Equation (3.1.1a) by p to get the first condition and divide Equation (3.1.1c) by p to get the second condition. □

Lemma 3.4.11. *If $p \nmid b_1$, $p \mid b_2$ and Equation System (3.1.1) has a non trivial solution in $\mathbb{Q}_p$, then:*

$$\begin{cases} \left(\dfrac{-\overline{b_2}\overline{e_2}}{p}\right) = 1, \\ \left(\dfrac{-b_1\overline{b_2}\overline{e_3}}{p}\right) = 1. \end{cases}$$

Proof. The proof of this lemma is practically identical to the proof of Lemma 3.4.10 with two differences caused by the change of p-valuation of b_1 and b_2.

When $p \nmid b_1$ and $p \mid b_2$, Equation (3.1.1a) implies a condition on b_2 instead of b_1.

Also, we study Equation (3.1.1b) instead of (3.1.1c) for the second condition. □

Lemma 3.4.12. *If $p \mid b_1$, $p \mid b_2$ and Equation System (3.1.1) has a non trivial solution in $\mathbb{Q}_p$, then:*

$$\begin{cases} \left(\dfrac{\overline{b_1}\overline{e_3}}{p}\right) = 1, \\ \left(\dfrac{\overline{b_2}\overline{(e_3 - e_2)}}{p}\right) = 1. \end{cases}$$

Proof. If $p \mid z_1$ or $p \mid d$, Equation (3.1.1b) implies that p divides both. Equation (3.1.1c) then implies that $p \mid z_3$ and then that $p \mid z_2$. Since $GCD(z_1,z_2,z_3,d) = 1$, this means that $p \nmid z_1 d$.

If $p \mid z_2$, Equation (3.1.1c) implies that $p \mid d$ and this is not possible from the preceding argument. This means that $p \nmid z_1 z_2 d$.

We can then divide Equation (3.1.1b) by p to get the first condition and divide Equation (3.1.1c) by p to get the second condition. □

The combination of the above lemmas forms our conditions in the case where $p \mid\mid e_2$, $p \mid\mid e_3$ and $p \mid\mid (e_3 - e_2)$.

3.4.2.5. Proofs when $p^2 \mid e_2$, $p \mid\mid e_3$ and $p \mid\mid (e_3 - e_2)$:

Lemma 3.4.13. *If $v_p(e_2) \equiv_2 0$, $p \nmid b_1$, $p \nmid b_2$ and Equation System (3.1.1) has a non trivial solution in $\mathbb{Q}_p$, then:*

$$\begin{cases} \left(\dfrac{b_1}{p}\right) = 1, \\ \left(\dfrac{b_2}{p}\right) = 1. \end{cases}$$

Proof. First, we remark that as soon as $p \mid z_i$ for some i, $p \mid z_j$ for all j. So we need $p \nmid z_1 z_2 z_3$.

The first condition then comes from Equation (3.1.1c) while the second condition then comes from Equation (3.1.1b). □

Lemma 3.4.14. *If $v_p(e_2) \equiv_2 0$, $p \mid b_1$, $p \nmid b_2$ and Equation System (3.1.1) has a non trivial solution in $\mathbb{Q}_p$, then:*

$$\begin{cases} \left(\dfrac{-b_2\overline{e_2}}{p}\right) = 1, \\ \left(\dfrac{-\overline{b_1}b_2\overline{e_3}}{p}\right) = 1. \end{cases}$$

Proof. In order for Equation (3.1.1a) to have a solution, we need that $p \mid z_2$. We then get that $p \mid z_1$ for the same reason. If $p \mid z_3$ or $p \mid d$, the p-valuations of the terms in Equation (3.1.1b) imply that p divides both. Since $GCD(z_1,z_2,z_3,d) = 1$, $p \nmid z_3 d$.

The p-valuations of the terms in Equation (3.1.1a) imply that $p^{v_p(e_2)/2} \mid z_1$ and $p^{v_p(e_2)/2} \mid\mid z_2$. We can then divide Equation (3.1.1a) by $p^{v_p(e_2)}$ to get the first condition.

We can then divide Equation (3.1.1b) by p to get the second condition. □

Lemma 3.4.15. *If $v_p(e_2) \equiv_2 0$, $p \nmid b_1$, $p \mid b_2$ and Equation System (3.1.1) has a non trivial solution in $\mathbb{Q}_p$, then:*

$$\begin{cases} \left(\dfrac{b_1\overline{e_2}}{p}\right) = 1, \\ \left(\dfrac{-b_1\overline{b_2}\overline{e_3}}{p}\right) = 1. \end{cases}$$

Proof. In order for Equation (3.1.1a) to have a solution, we need that $p \mid z_1$. We then get that $p \mid z_2$ for the same reason. If $p \mid z_3$ or $p \mid d$, the p-valuations of the terms in Equation (3.1.1b) imply that p divides both. Since $GCD(z_1,z_2,z_3,d) = 1$, $p \nmid z_3 d$.

The p-valuations of the terms in Equation (3.1.1a) imply that $p^{v_p(e_2)/2} \mid\mid z_1$ and $p^{v_p(e_2)/2} \mid z_2$. We then divide Equation (3.1.1a) by $p^{v_p(e_2)}$ to get the first condition

We can then divide Equation (3.1.1b) by p to get the second condition. □

Lemma 3.4.16. *If $v_p(e_2) \equiv_2 0$, $p \mid b_1$, $p \mid b_2$ and Equation System (3.1.1) has a non trivial solution in $\mathbb{Q}_p$, then:*

$$\begin{cases} \left(\dfrac{\overline{b_1 b_2}}{p}\right) = 1, \\ \left(\dfrac{\overline{b_1}\overline{e_3}}{p}\right) = 1. \end{cases}$$

Proof. First, we start by dividing all equations by p and working in $\mathbb{Z}/p\mathbb{Z}$.

The first condition then comes from Equation (3.1.1a).

The second condition then comes from Equation (3.1.1b). □

Lemma 3.4.17. *If $v_p(e_2) \equiv_2 1$, $p \nmid b_1$, $p \nmid b_2$ and Equation System (3.1.1) has a non trivial solution in $\mathbb{Q}_p$, then:*

$$\begin{cases} \left(\dfrac{b_1}{p}\right) = 1, \\ \left(\dfrac{b_2}{p}\right) = 1. \end{cases}$$

Proof. First, we remark that as soon as $p \mid z_i$ for some i, $p \mid z_j$ for all j. So we need $p \nmid z_1 z_2 z_3$.

The first condition then comes from Equation (3.1.1c).

The second condition then comes from Equation (3.1.1b). □

Lemma 3.4.18. *If $v_p(e_2) \equiv_2 1$, $p \mid b_1$, $p \nmid b_2$ and Equation System (3.1.1) has a non trivial solution in $\mathbb{Q}_p$, then:*

$$\begin{cases} \left(\dfrac{\overline{b_1}\overline{e_2}}{p}\right) = 1, \\ \left(\dfrac{-\overline{b_1}b_2\overline{e_3}}{p}\right) = 1. \end{cases}$$

Proof. This proof is very similar to the proof of Lemma 3.4.11.

In order for Equation (3.1.1a) to have a solution, we need that $p \mid z_2$. We then get that $p \mid z_1$ for the same reason. If $p \mid z_3$ or $p \mid d$, the p-valuations of the terms in Equation (3.1.1b) imply that p divides both. Since $GCD(z_1,z_2,z_3,d) = 1$, $p \nmid z_3d$.

The p-valuations of the terms in Equation (3.1.1a) imply that $p^{(v_p(e_2)-1)/2} \mid\mid z_1$ and $p^{(v_p(e_2)+1)/2} \mid z_2$. We then divide Equation (3.1.1a) by $p^{v_p(e_2)}$ to get the first condition.

We can then divide Equation (3.1.1b) by p to get the second condition. □

Lemma 3.4.19. *If $v_p(e_2) \equiv_2 1$, $p \nmid b_1$, $p \mid b_2$ and Equation System (3.1.1) has a non trivial solution in $\mathbb{Q}_p$, then:*

$$\begin{cases} \left(\dfrac{-\overline{b_2}\overline{e_2}}{p}\right) = 1, \\ \left(\dfrac{-\overline{b_1}b_2\overline{e_3}}{p}\right) = 1. \end{cases}$$

Proof. The proof of this lemma is practically identical to the proof of Lemma 3.4.18 with the new of p-valuation of b_1 and b_2 changing the first condition. □

Lemma 3.4.20. *If $v_p(e_2) \equiv_2 1$, $p \mid b_1$, $p \mid b_2$ and Equation System (3.1.1) has a non trivial solution in $\mathbb{Q}_p$, then:*

$$\begin{cases} \left(\dfrac{\overline{b_1 b_2}}{p}\right) = 1, \\ \left(\dfrac{\overline{b_1}\overline{e_3}}{p}\right) = 1. \end{cases}$$

Proof. First, we start by dividing all equations by p and working in $\mathbb{Z}/p\mathbb{Z}$.

The first condition then comes from Equation (3.1.1a).

The second condition then comes from Equation (3.1.1b). □

The combination of the above lemmas forms our conditions in the case where $p^2 \mid e_2$, $p \mid\mid e_3$ and $p \mid\mid (e_3 - e_2)$.

3.4.2.6. Proofs when $p \mid\mid e_2$, $p^2 \mid e_3$ and $p \mid\mid (e_3 - e_2)$:

Lemma 3.4.21. *If $v_p(e_3) \equiv_2 0$, $p \nmid b_1$, $p \nmid b_2$ and Equation System (3.1.1) has a non trivial solution in $\mathbb{Q}_p$, then:*

$$\begin{cases} \left(\dfrac{b_1}{p}\right) = 1, \\ \left(\dfrac{b_2}{p}\right) = 1. \end{cases}$$

Proof. First, we remark that as soon as $p \mid z_i$ for some i, $p \mid z_j$ for all j. So we need $p \nmid z_1 z_2 z_3$.

The first condition then comes from Equation (3.1.1c).

The second condition then comes from Equation (3.1.1b). □

Lemma 3.4.22. *If $v_p(e_3) \equiv_2 0$, $p \mid b_1$, $p \nmid b_2$ and Equation System (3.1.1) has a non trivial solution in $\mathbb{Q}_p$, then:*

$$\begin{cases} \left(\dfrac{\overline{b_1}\overline{e_2}}{p}\right) = 1, \\ \left(\dfrac{b_2}{p}\right) = 1. \end{cases}$$

Proof. In order for Equation (3.1.1a) to have a solution, we need that $p \mid z_2$.

If $p \mid z_1$ or $p \mid d$, Equation (3.1.1a) implies that p divides both. Equation (3.1.1b) then implies that $p \mid z_3$ but this is impossible since $GCD(z_1,z_2,z_3,d) = 1$. This means that $p \nmid z_1,d$.

If $p \mid z_3$, Equation (3.1.1c) implies that $p \mid d$ but we have already shown that this is impossible. It follows that $p \nmid z_3$.

We can then divide Equation (3.1.1a) by p to get the first condition and divide Equation (3.1.1b) by p to get the second condition. □

Lemma 3.4.23. *If $v_p(e_3) \equiv_2 0$, $p \nmid b_1$, $p \mid b_2$ and Equation System (3.1.1) has a non trivial solution in $\mathbb{Q}_p$, then:*

$$\begin{cases} \left(\dfrac{-\overline{b_2}\overline{e_2}}{p}\right) = 1, \\ \left(\dfrac{b_1\overline{e_3}}{p}\right) = 1. \end{cases}$$

Proof. In order for Equation (3.1.1a) to have a solution, we need that $p \mid z_1$.

If $p \mid z_2$ or $p \mid d$, Equation (3.1.1a) implies that p divides both. Equation (3.1.1b) would then imply that $p \mid z_3$ but this is impossible since $GCD(z_1,z_2,z_3,d) = 1$. This means that $p \nmid z_2,d$.

We can then divide Equation (3.1.1a) by p to get the first condition.

The p-valuations of the terms in Equation (3.1.1b) imply that $p^{v_p(e_3)/2} \mid\mid z_1$ and $p^{v_p(e_3)/2} \mid z_3$. We can then divide Equation (3.1.1b) by $p^{v_p(e_3)}$ to get the second condition. □

Lemma 3.4.24. *If $v_p(e_3) \equiv_2 0$, $p \mid b_1$, $p \mid b_2$ and Equation System (3.1.1) has a non trivial solution in $\mathbb{Q}_p$, then:*

$$\begin{cases} \left(\dfrac{\overline{b_2}\overline{(e_3 - e_2)}}{p}\right) = 1, \\ \left(\dfrac{-\overline{b_1b_2}\overline{e_3}}{p}\right) = 1. \end{cases}$$

PROOF. If $p \mid z_2$ or $p \mid d$, Equation (3.1.1c) implies that p divides both and then that $p \mid z_3$. Equation (3.1.1a) then implies that $p \mid z_1$. Since $GCD(z_1,z_2,z_3,d) = 1$, this means that $p \nmid z_2 d$.

We can then divide Equation (3.1.1c) by p to get the first condition.

The p-valuations of the terms in Equation (3.1.1b) imply that $p^{v_p(e_3)/2} \mid z_1$ and $p^{v_p(e_3)/2-1} \mid\mid z_3$. We can then divide Equation (3.1.1b) by $p^{v_p(e_3)}$ to get the second condition. □

Lemma 3.4.25. *If $v_p(e_3) \equiv_2 1$, $p \nmid b_1$, $p \nmid b_2$ and Equation System (3.1.1) has a non trivial solution in $\mathbb{Q}_p$, then:*

$$\begin{cases} \left(\dfrac{b_1}{p}\right) = 1, \\ \left(\dfrac{b_2}{p}\right) = 1. \end{cases}$$

PROOF. First, we remark that as soon as $p \mid z_i$ for some i, $p \mid z_j$ for all j. So we need $p \nmid z_1 z_2 z_3$.

The first condition then comes from Equation (3.1.1c).

The second condition then comes from Equation (3.1.1b). □

Lemma 3.4.26. *If $v_p(e_3) \equiv_2 1$, $p \mid b_1$, $p \nmid b_2$ and Equation System (3.1.1) has a non trivial solution in $\mathbb{Q}_p$, then:*

$$\begin{cases} \left(\dfrac{\overline{b_1}\overline{e_2}}{p}\right) = 1, \\ \left(\dfrac{b_2}{p}\right) = 1. \end{cases}$$

PROOF. In order for Equation (3.1.1a) to have a solution, we need that $p \mid z_2$.

If $p \mid z_1$ or $p \mid d$, Equation (3.1.1a) implies that p divides both. Equation (3.1.1b) then implies that $p \mid z_3$ but this is impossible since $GCD(z_1,z_2,z_3,d) = 1$. This means that $p \nmid z_1,d$.

If $p \mid z_3$, Equation (3.1.1c) implies that $p \mid d$ but we have already shown that this is impossible. It follows that $p \nmid z_3$.

We can then divide Equation (3.1.1a) by p to get the first condition and divide Equation (3.1.1b) by p to get the second condition. □

Lemma 3.4.27. *If $v_p(e_3) \equiv_2 1$, $p \nmid b_1$, $p \mid b_2$ and Equation System (3.1.1) has a non trivial solution in $\mathbb{Q}_p$, then:*

$$\begin{cases} \left(\dfrac{-\overline{b_2}\,\overline{e_2}}{p}\right) = 1, \\ \left(\dfrac{-b_1\overline{b_2}\,\overline{e_3}}{p}\right) = 1. \end{cases}$$

Proof. In order for Equation (3.1.1a) to have a solution, we need that $p \mid z_1$.

If $p \mid z_2$ or $p \mid d$, Equation (3.1.1a) implies that p divides both. Equation (3.1.1b) would then imply that $p \mid z_3$ but this is impossible since $GCD(z_1,z_2,z_3,d) = 1$. This means that $p \nmid z_2,d$.

We can then divide Equation (3.1.1a) by p to get the first condition.

The p-valuations of the terms in Equation (3.1.1b) imply that $p^{v_p(e_3)/2+1} \mid z_1$ and $p^{(v_p(e_3)-1)/2} \mid\mid z_3$. We can then divide Equation (3.1.1b) by $p^{v_p(e_3)}$ to get the second condition. □

Lemma 3.4.28. *If $v_p(e_3) \equiv_2 1$, $p \mid b_1$, $p \mid b_2$ and Equation System (3.1.1) has a non trivial solution in $\mathbb{Q}_p$, then:*

$$\begin{cases} \left(\dfrac{\overline{b_2}\,\overline{(e_3 - e_2)}}{p}\right) = 1, \\ \left(\dfrac{\overline{b_1}\,\overline{e_3}}{p}\right) = 1. \end{cases}$$

Proof. If $p \mid z_2$ or $p \mid d$, Equation (3.1.1c) implies that p divides both and then that $p \mid z_3$. Equation (3.1.1a) then implies that $p \mid z_1$. Since $GCD(z_1,z_2,z_3,d) = 1$, this means that $p \nmid z_2 d$.

We can then divide Equation (3.1.1c) by p to get the first condition.

The p-valuations of the terms in Equation (3.1.1b) imply that $p^{(v_p(e_3)-1)/2} \mid\mid z_1$ and $p^{(v_p(e_3)-1)/2} \mid z_3$. We can then divide Equation (3.1.1b) by $p^{v_p(e_3)}$ to get the second condition. □

The combination of the above lemmas forms our conditions in the case where $p \mid\mid e_2$, $p^2 \mid e_3$ and $p \mid\mid (e_3 - e_2)$.

3.4.2.7. Proofs when $p \mid\mid e_2$, $p \mid\mid e_3$ and $p^2 \mid (e_3 - e_2)$: If we exchange Equation (3.1.1b) with Equation (3.1.1c), we remark that we can write the equation system as:

$$\begin{cases} b_2 z_2^2 - b_1 z_1^2 = (-e_2)d^2, \\ b_2 z_2^2 - b_1 b_2 z_3^2 = (e_3 - e_2)d^2, \\ b_1 z_1^2 - b_1 b_2 z_3^2 = ((e_3 - e_2) - (-e_2))d^2, \end{cases}$$

which is simply a system that respects the conditions of our original system but with $e_2 \mapsto -e_2$, $e_3 \mapsto (e_3 - e_2)$, $b_1 \rightleftarrows b_2$ and $z_1 \rightleftarrows z_2$.

We can then simply use the proofs of the case where $p \mid\mid e_2$, $p^2 \mid e_3$ and $p \mid\mid (e_3 - e_2)$.

3.4.3. The proofs of sufficiency

As in the case for $\mathbb{Q}_2$, sufficient conditions are not relevant for the results of this thesis. In addition, our proofs of sufficiency are very similar to each other. Because of this, we will explain the general idea of the proofs but do only one of them explicitly.

The idea is to show that the conditions are sufficient in $\mathbb{Z}/p^m\mathbb{Z}$ for a big enough m. This can be done by simply finding a solution. We can then apply Hensel's Lemma on two of the variables to prove that there is a solution in $\mathbb{Q}_p$.

As an example, here is one of the proofs:

Proposition 3.4.29. *If $p \mid\mid e_2$,e_3,$(e_3 - e_2)$, then the conditions given by Theorem 3.4.2 are sufficient to guarantee a non-trivial solution for Equation System (3.1.1) in $\mathbb{Q}_p$.*

Proof. Let b_1 and b_2 be two square-free integers respecting the conditions given by Theorem 3.4.2. We separate this proof in four cases depending on the valuation of b_1,b_2:

Case 1. If $p \nmid b_1$ and $p \nmid b_2$, we will show that there is a solution in $\mathbb{Z}/p\mathbb{Z}$. Since the conditions in Theorem 3.4.2 imply that $\left(\frac{b_1}{p}\right) = \left(\frac{b_2}{p}\right) = 1$, there are k_1, k_2 such that $k_1^2 \equiv_p b_1$ and $k_2^2 \equiv_p b_2$. We can then take $d = p$, $z_3 = 1$, $z_1 = k_2$ and $z_2 = k_1$ and this yields a solution with $b_1 z_1^2 \not\equiv_p 0 \not\equiv_p b_2 z_2^2$.

Once we have a solution in $\mathbb{Z}/p\mathbb{Z}$ we can apply Hensel's Lemma to z_1 in Equation (3.1.1b) and then reapply Hensel's Lemma to z_2 in Equation 3.1.1c. Since each variable does not appear in the other equation, we have a solution in $\mathbb{Q}_p$.

Case 2. If $p \nmid b_1$ and $p \mid b_2$, we will show that there is a solution in $\mathbb{Z}/p^2\mathbb{Z}$. Since the conditions in Theorem 3.4.2 imply that $\left(\frac{\overline{-b_1 b_2 e_3}}{p}\right) = \left(\frac{\overline{-b_2 e_2}}{p}\right) = 1$, there are k_1, k_2 such that $k_1^2 \equiv_p -\overline{e_3}\,\overline{b_1 b_2}^{-1}$ and $k_2^2 \equiv_p -\overline{e_2}\,\overline{b_2}^{-1}$. We can then take $z_1 = p$, $d = 1$, $z_2 = k_2$ and $z_3 = k_1$. We can then divide every equation by p to see that it is a solution in $\mathbb{Z}/p\mathbb{Z}$ with $\frac{b_2 z_2^2}{p} \not\equiv_p 0 \not\equiv_p \frac{b_1 b_2 z_3^2}{p}$.

Once we have a solution in $\mathbb{Z}/p^2\mathbb{Z}$ we can apply Hensel's Lemma to z_2 in Equation (3.1.1a) and then reapply Hensel's Lemma to z_3 in Equation 3.1.1b. Since each variable does not appear in the other equation, we have a solution in $\mathbb{Q}_p$.

Case 3. If $p \mid b_1$ and $p \nmid b_2$, we will show that there is a solution in $\mathbb{Z}/p^2\mathbb{Z}$. Since the conditions in Theorem 3.4.2 imply that $\left(\frac{\overline{-b_1 b_2 (e_3 - e_2)}}{p}\right) = \left(\frac{\overline{b_1 e_2}}{p}\right) = 1$, there are k_1, k_2 such that $k_1^2 \equiv_p -\overline{(e_3 - e_2)}\,\overline{b_1 b_2}^{-1}$ and $k_2^2 \equiv_p \overline{e_2}\,\overline{b_1}^{-1}$. We can then take $z_2 = p$, $d = 1$, $z_1 = k_2$ and $z_3 = k_1$. We can then divide every equation by p to see that it is a solution in $\mathbb{Z}/p\mathbb{Z}$ with $\frac{b_1 z_1^2}{p} \not\equiv_p 0 \not\equiv_p \frac{b_1 b_2 z_3^2}{p}$.

Once we have a solution in $\mathbb{Z}/p^2\mathbb{Z}$ we can apply Hensel's Lemma to z_1 in Equation (3.1.1a) and then reapply Hensel's Lemma to z_3 in Equation 3.1.1c. Since each variable does not appear in the other equation, we have a solution in $\mathbb{Q}_p$.

Case 4. If $p \mid b_1$ and $p \mid b_2$, we will show that there is a solution in $\mathbb{Z}/p^2\mathbb{Z}$. Since the conditions in Theorem 3.4.2 imply that $\left(\frac{\overline{b_1 e_3}}{p}\right) = \left(\frac{\overline{b_2 (e_3 - e_2)}}{p}\right) = 1$, there are k_1, k_2 such that $k_1^2 \equiv_p \overline{e_3}\,\overline{b_1}^{-1}$ and $k_2^2 \equiv_p \overline{(e_3 - e_2)}\,\overline{b_2}^{-1}$. We can then take $z_1 = k_1$, $d = 1$, $z_2 = k_2$ and $z_3 = p$. We can then divide every equation by p to see that it is a solution in $\mathbb{Z}/p\mathbb{Z}$ with $\frac{b_1 z_1^2}{p} \not\equiv_p 0 \not\equiv_p \frac{b_2 z_2^2}{p}$.

Once we have a solution in $\mathbb{Z}/p^2\mathbb{Z}$ we can apply Hensel's Lemma to z_1 in Equation (3.1.1b) and then reapply Hensel's Lemma to z_2 in Equation 3.1.1c. Since each variable does not appear in the other equation, we have a solution in $\mathbb{Q}_p$. □

Chapter 4

Construction of the Generalized Monsky Matrix

4.1. Reparametrization of $(b_1{,}b_2)$

Now that we have all the conditions for a local solution, we will construct a matrix whose kernel is in correspondence with the pairs $(b_1{,}b_2)$ respecting our conditions from Theorems 3.2.1, 3.3.1, 3.3.2, 3.3.3, 3.3.4, 3.4.1 and 3.4.2. To achieve this, we first need to write the pairs in a way that they can be transformed by a matrix. More precisely, we will write them as vectors with parameters in $\mathbb{Z}/2\mathbb{Z}$.

In order to do this, we start by factorizing the roots of the elliptic curve:

$$\begin{cases} e_2 = \pm 2^{v_2(e_2)} \left(\prod_{i=1}^{n_1} p_{1_i}\right) \left(\prod_{i=1}^{n_2} p_{2_i}^{v_{p_{2_i}}(e_2)}\right) \left(\prod_{i=1}^{n_3} p_{3_i}\right) \left(\prod_{i=1}^{n_4} p_{4_i}\right) \left(\prod_{i=1}^{n_5} p_{5_i}^{v_{p_{5_i}}(e_2)}\right), \\ e_3 = \pm 2^{v_2(e_3)} \left(\prod_{i=1}^{n_1} p_{1_i}\right) \left(\prod_{i=1}^{n_2} p_{2_i}\right) \left(\prod_{i=1}^{n_3} p_{3_i}^{v_{p_{3_i}}(e_3)}\right) \left(\prod_{i=1}^{n_4} p_{4_i}\right) \left(\prod_{i=1}^{n_6} p_{6_i}^{v_{p_{6_i}}(e_3)}\right), \\ e_3 - e_2 = \pm 2^{v_2(e_3-e_2)} \left(\prod_{i=1}^{n_1} p_{1_i}\right) \left(\prod_{i=1}^{n_2} p_{2_i}\right) \left(\prod_{i=1}^{n_3} p_{3_i}\right) \left(\prod_{i=1}^{n_4} p_{4_i}^{v_{p_{4_i}}(e_3-e_2)}\right) \left(\prod_{i=1}^{n_7} p_{7_i}^{v_{p_{7_i}}(e_3-e_2)}\right), \end{cases}$$

with our odd primes separated into seven categories:

(1) The primes p_{1_i} that exactly divide e_2, e_3 and $(e_3 - e_2)$.

(2) The primes p_{2_i} that exactly divide e_3 and $(e_3 - e_2)$ and whose squares divide e_2.

(3) The primes p_{3_i} that exactly divide e_2 and $(e_3 - e_2)$ and whose squares divide e_3.

(4) The primes p_{4_i} that exactly divide e_2 and e_3 and whose squares divide $(e_3 - e_2)$.

(5) The primes p_{5_i} that only divide e_2.

(6) The primes p_{6_i} that only divide e_3.

(7) The primes p_{7_i} that only divide $(e_3 - e_2)$.

Using this notation, we can write the pair (b_1,b_2) as:

$$\begin{cases} b_1 = (-1)^{\delta_1} 2^{\epsilon_1} \left(\prod_{j=1}^{4} \prod_{i=1}^{n_j} p_{j_i}^{\alpha_{j_i}} \right) \left(\prod_{i=1}^{n_5} p_{5_i}^{\gamma_i} \right) \left(\prod_{i=1}^{n_6} p_{6_i}^{\alpha_{6_i}} \right), \\ b_2 = (-1)^{\delta_2} 2^{\epsilon_2} \left(\prod_{j=1}^{4} \prod_{i=1}^{n_j} p_{j_i}^{\beta_{j_i}} \right) \left(\prod_{i=1}^{n_5} p_{5_i}^{\gamma_i} \right) \left(\prod_{i=1}^{n_7} p_{7_i}^{\beta_{7_i}} \right), \end{cases} \tag{4.1.1}$$

with all the exponents either 0 or 1 since $b_1,b_2 \in \mathbb{Q}^\times/\mathbb{Q}^{\times^2}$.

We remark here that primes of Category 5 have to divide either none or both of the b_i's because of the conditions of Theorem 3.4.1. Likewise, primes of Category 6 cannot divide b_2 and primes of Category 7 cannot divide b_1.

Consider the group $\mathbb{Q}(S,2) \times \mathbb{Q}(S,2)$ as defined in Theorem 2.5.3 and define its subgroup H by only taking the pairs (b_1,b_2) respecting the properties that we have just explained for primes of Categories 1, 2 and 3.

We have the following group isomorphism f:

$$\begin{aligned} f : H &\to (\mathbb{Z}/2\mathbb{Z})^{2n_1+2n_2+2n_3+2n_4+n_5+n_6+n_7+4} \\ (b_1,b_2) &\mapsto \left(\begin{array}{ccccc|ccc|ccccc} \delta_1 & \epsilon_1 & \alpha_{1_1} & \dots & \alpha_{6_{n_6}} & \gamma_1 & \dots & \gamma_{n_5} & \delta_2 & \epsilon_2 & \beta_{1_1} & \dots & \beta_{7_{n_7}} \end{array} \right) \end{aligned}$$

We remark here that there is no α_{5_i} or β_{5_i} since we decided to call these exponents γ_i to avoid confusion as they appear in both b_1 and b_2. We also note that we separate the parameters in 3 parts: the first part represents the exponents appearing only for b_1 (noted above by the α's), the second part represents the exponents appearing for both b_1 and b_2 (noted above by the γ's), the third part represents the exponents appearing only for b_2 (noted above by the β's).

To simplify the notation, we write $m_1 = 2 + n_1 + n_2 + n_3 + n_4 + n_6$, $m_2 = 2 + n_1 + n_2 + n_3 + n_4 + n_7$ and $m_3 = n_5$. We also rename our factors as follows:

$$q_{1_j} = \begin{cases} -1 \text{ if } j = 1, \\ 2 \text{ if } j = 2, \\ p_{1_{j-2}} \text{ if } 3 \leq j \leq 2 + n_1, \\ p_{2_{j-2-n_1}} \text{ if } 3 + n_1 \leq j \leq 2 + n_1 + n_2, \\ p_{3_{j-2-n_1-n_2}} \text{ if } 3 + n_1 + n_2 \leq j \leq 2 + n_1 + n_2 + n_3, \\ p_{4_{j-2-n_1-n_2-n_3}} \text{ if } 3 + n_1 + n_2 + n_3 \leq j \leq 2 + n_1 + n_2 + n_3 + n_4, \\ p_{6_{j-2-n_1-n_2-n_3-n_4}} \text{ if } 3 + n_1 + n_2 + n_3 + n_4 \leq j \leq m_1. \end{cases}$$

$$q_{2_j} = \begin{cases} -1 \text{ if } j = 1, \\ 2 \text{ if } j = 2, \\ p_{1_{j-2}} \text{ if } 3 \leq j \leq 2 + n_1, \\ p_{2_{j-2-n_1}} \text{ if } 3 + n_1 \leq j \leq 2 + n_1 + n_2, \\ p_{3_{j-2-n_1-n_2}} \text{ if } 3 + n_1 + n_2 \leq j \leq 2 + n_1 + n_2 + n_3, \\ p_{4_{j-2-n_1-n_2-n_3}} \text{ if } 3 + n_1 + n_2 + n_3 \leq j \leq 2 + n_1 + n_2 + n_3 + n_4, \\ p_{7_{j-2-n_1-n_2-n_3-n_4}} \text{ if } 3 + n_1 + n_2 + n_3 + n_4 \leq j \leq m_2. \end{cases}$$

$$q_{3_j} = \begin{cases} p_{5_j} \text{ for all } j. \end{cases}$$

With this new notation, we can rewrite b_1 and b_2 as:

$$\begin{cases} b_1 = \left(\prod_{j=1}^{m_1} q_{1_j}^{\omega_{1_j}} \right) \left(\prod_{j=1}^{m_3} q_{3_j}^{\omega_{3_j}} \right), \\ b_2 = \left(\prod_{j=1}^{m_2} q_{2_j}^{\omega_{2_j}} \right) \left(\prod_{j=1}^{m_3} q_{3_j}^{\omega_{3_j}} \right), \end{cases} \tag{4.1.2}$$

with all the exponents either 0 or 1 since b_1,$b_2 \in \mathbb{Q}^\times / \mathbb{Q}^{\times^2}$.

We can also rewrite f as:

$$\begin{aligned}
&f : H \to (\mathbb{Z}/2\mathbb{Z})^{m_1+m_2+m_3}\\
&(b_1,b_2) \mapsto \left(\begin{array}{ccccc|ccc|ccccc} \omega_{1_1} & \omega_{1_2} & \omega_{1_3} & \dots & \omega_{1_{m_1}} & \omega_{3_1} & \dots & \omega_{3_{m_3}} & \omega_{2_1} & \omega_{2_2} & \omega_{2_3} & \dots & \omega_{2_{m_2}} \end{array} \right)
\end{aligned}$$

With this new parameterization, we interpret our pairs (b_1,b_2) as vectors. The goal of this chapter is to create a matrix whose kernel is the set of pairs (b_1,b_2) (seen as vectors) that respect all local conditions from Chapter 3.

More precisely, we want to find a matrix M with parameters in $\mathbb{Z}/2\mathbb{Z}$ such that:

$$f((b_1,b_2))^t \in \ker(M) \iff (b_1,b_2) \text{ respects all local conditions.}$$

In order to make this more readable, we will separate the matrix in three parts: the row representing the condition on $\mathbb{R}$, the rows representing the conditions on $\mathbb{Q}_2$ and the rows representing the conditions on $\mathbb{Q}_p$.

4.2. Matrix row for $\mathbb{R}$

When e_2 and e_3 are fixed, there is only one condition for a solution in $\mathbb{R}$. Let us call this one row matrix $M_{\mathbb{R}}$.

Before giving the matrix, we start by defining some basic submatrices that we will use as the building blocks of $M_{\mathbb{R}}$.

Definition 4.2.1. *For $i \in \{1,2\}$, we define S_i as:*

$$S_i = (s_{1,j}) \textit{ for } 1 \le j \le m_i,$$

$$s_{1,j} = \begin{cases} 1 & \textit{if } j = 1, \\ 0 & \textit{otherwise.} \end{cases}$$

The role of S_i is to check the sign of b_i.

Definition 4.2.2. *The matrix $O_{i,j}$ is the zero matrix with i lines and j columns.*

This last submatrix will be used for several parts in the final matrix.

We now get to $M_{\mathbb{R}}$. We will separate the cases on e_2 and e_3 as in Theorem 3.2.1.

Lemma 4.2.3. *If $e_2 > 0$ and $e_3 > 0$, the local conditions on $\mathbb{R}$ can be represented by:*

$$M_{\mathbb{R}} = \left(\begin{array}{c|c|c} S_1 & O_{1,n_5} & O_{1,m_2} \end{array} \right).$$

Proof. We remark here that $M_{\mathbb{R}}$ has exactly one non-zero component and it is in the position representing the variable ω_{1_1} of Equation (4.1.2). Because of this, $M_{\mathbb{R}} f((b_1,b_2))^t = (\omega_{1_1})$. This means that $f((b_1,b_2))^t \in \ker(M_{\mathbb{R}})$ if and only if $\omega_{1_1} = 0$ and this is true if and only if $b_1 > 0$ which is the required condition from Theorem 3.2.1. □

Lemma 4.2.4. *If $e_2 < 0$ and $e_3 - e_2 > 0$, the local conditions on $\mathbb{R}$ can be represented by:*

$$M_{\mathbb{R}} = \left(\begin{array}{c|c|c} O_{1,m_1} & O_{1,n_5} & S_2 \end{array} \right).$$

Proof. We remark here that $M_{\mathbb{R}}$ has exactly one non-zero component and it is in the position representing the variable ω_{2_1}. Because of this, $M_{\mathbb{R}} f((b_1,b_2))^t = (\omega_{2_1})$. This means that $f((b_1,b_2))^t \in \ker(M_{\mathbb{R}})$ if and only if $\omega_{2_1} = 0$ and this is true if and only if $b_2 > 0$ which is the required condition from Theorem 3.2.1. □

Lemma 4.2.5. *If $e_3 < 0$ and $e_3 - e_2 < 0$, the local conditions on $\mathbb{R}$ can be represented by:*

$$M_{\mathbb{R}} = \left(\begin{array}{c|c|c} S_1 & O_{1,n_5} & S_2 \end{array} \right).$$

Proof. We remark here that $M_{\mathbb{R}}$ has exactly two non-zero components and they are in the positions representing ω_{1_1} and ω_{2_1}. Because of this, $M_{\mathbb{R}} f((b_1,b_2))^t = (\omega_{1_1} + \omega_{2_1})$. This means that $f((b_1,b_2))^t \in \ker(M_{\mathbb{R}})$ if and only if $\omega_{1_1} + \omega_{2_1} \equiv_2 0$ and this is true if and only if $b_1 b_2 > 0$ which is the required condition from Theorem 3.2.1. □

Lemmas 4.2.3, 4.2.4 and 4.2.5 codify the statement of Theorem 3.2.1.

4.3. Matrix rows for $\mathbb{Q}_2$

When e_2 and e_3 are fixed, there are three conditions for a solution in $\mathbb{Q}_2$. Let us call this submatrix $M_{\mathbb{Q}_2}$.

As in the preceding case, we start by defining the building blocks needed to construct the submatrix.

Definition 4.3.1. *For $i \in \{1{,}2\}$, we define R_i as:*

$$R_i = (r_{1,j}) \textit{ for } 1 \leq j \leq m_i,$$
$$r_{1,j} = \begin{cases} 1 \textit{ if } j = 2, \\ 0 \textit{ otherwise.} \end{cases}$$

The role of R_i is to check if $2 \mid b_i$.

Definition 4.3.2. *For $i \in \{1{,}2\}$ and $k \in \{3{,}5{,}7\}$, we define $T_{i,k}$ as:*

$$T_{i,k} = (t_{1,j}) \textit{ for } 1 \leq j \leq m_i,$$
$$t_{1,j} = \begin{cases} 0 \textit{ if } j = 2, \\ 0 \textit{ if } q_{i_j} \equiv_8 1 \textit{ or } k, \\ 1 \textit{ otherwise.} \end{cases}$$

Definition 4.3.3. *For $k \in \{3{,}5{,}7\}$, we define $T_{3,k}$ as:*

$$T_{3,k} = (t_{1,j}) \textit{ for } 1 \leq j \leq m_3,$$
$$t_{1,j} = \begin{cases} 0 \textit{ if } q_{3_j} \equiv_8 1 \textit{ or } k, \\ 1 \textit{ otherwise.} \end{cases}$$

When combined, the roles of $T_{i,k}$ and $T_{3,k}$ are to check if $b_i \equiv_8 1$ or k.

Also, in order to avoid considering 80 cases, we will introduce the following function:

Definition 4.3.4. *Let $S \subset (\mathbb{Z}/8\mathbb{Z})^\times$, and let a be an integer. If $\overline{a} = \frac{a}{2^{v_2(a)}}$ is seen as an element of $(\mathbb{Z}/8\mathbb{Z})^\times$, we define:*

$$\chi_S(a) = \begin{cases} 1 \textit{ if } \overline{a} \in S, \\ 0 \textit{ otherwise.} \end{cases}$$

We now define $M_{\mathbb{Q}_2}$. In order to make the submatrices readable, we will separate the cases by the valuations of e_2 and e_3. Also, since we explained $M_{\mathbb{R}}$ in detail and the arguments for each of the $M_{\mathbb{Q}_2}$ are all similar, we will do one of the $\mathbb{Q}_2$ cases in detail but then simply state the others.

Lemma 4.3.5. *If $2 \nmid e_3$ and $v_2(e_2) = 1$, we have that*

$$M_{\mathbb{Q}_2} = \left(\begin{array}{c|c|c} R_1 & O_{1,m_3} & R_2 \\ \hline \chi_{\{1,5\}}(e_3)T_{1,5} + \chi_{\{3,7\}}(e_2e_3)R_1 & T_{3,5} & \chi_{\{3,7\}}(e_3)T_{2,5} \\ \hline \begin{array}{c} \chi_{\{1,5\}}(e_2e_3)T_{1,7} \\ +\chi_{\{3,7\}}(e_2e_3)T_{1,3} \\ +\chi_{\{1,5\}}(e_2)\chi_{\{3,5\}}(e_3)R_1 + \chi_{\{3,7\}}(e_2)\chi_{\{1,3\}}(e_3)R_1 \end{array} & O_{1,m_3} & \begin{array}{c} \chi_{\{1,5\}}(e_2e_3)T_{2,7} \\ +\chi_{\{3,7\}}(e_2e_3)T_{2,3} \end{array} \end{array}\right).$$

Proof. As discussed in Section 3.3, when e_3 and e_2 are fixed, there are tree conditions each represented by one of the three rows.

For the first row, we remark that, as in the case of $M_{\mathbb{R}}$, when we multiply the row by $f((b_1,b_2))^t$, it gives $\omega_{1_2} + \omega_{2_2}$ and that gives 0 if and only if $2 \mid b_1 \iff 2 \mid b_2$. The first row then represents the first condition appearing in each cell of the table of Theorem 3.3.1.

The content of the second row depends on the values of $\overline{e_2}$ and $\overline{e_3}$ modulo 4. In the above matrix, the difference between the cases is represented by using the function χ.

If $\overline{e_2} \equiv_4 1$ and $\overline{e_3} \equiv_4 1$, then the only contributing terms in the second row are $T_{1,5}$ and $T_{3,5}$. The product of the second row by $f((b_1,b_2))^t$ gives

$$\sum_{\substack{1 \le j \le m_1 \\ j \ne 2}} \chi_{\{3,7\}}(q_{1_j})\omega_{1_j} + \sum_{1 \le j \le m_3} \chi_{\{3,7\}}(q_{3_j})\omega_{3_j}.$$

This number collects the sum of exponents corresponding to the prime factors of $\overline{b_1}$ that are congruent to 3 or 7 modulo 8. This sum is equal to 0 if and only if $\overline{b_1} \equiv_4 1$.

If $\overline{e_2} \equiv_4 1$ and $\overline{e_3} \equiv_4 3$, then the only contributing terms in the second row are those involving R_1, $T_{2,5}$ and $T_{3,5}$. The product of the second row by $f((b_1,b_2))^t$ gives

$$\omega_{1_2} + \sum_{\substack{1 \le j \le m_2 \\ j \ne 2}} \chi_{\{3,7\}}(q_{2_j})\omega_{2_j} + \sum_{1 \le j \le m_3} \chi_{\{3,7\}}(q_{3_j})\omega_{3_j}.$$

This number collects the sum of the exponents corresponding to the prime factors of $\overline{b_2}$ that are congruent to 3 or 7 modulo 8 and the 2-valuation of b_1. This sum is equal to 0 if and only if $(-1)^{v_2(b_1)}\overline{b_2} \equiv_4 1$. When $2 \nmid b_1$, the row represents the condition $\overline{b_2} \equiv_4 1$. When $2 \mid b_1$, the row represents the condition $-\overline{b_2} \equiv_4 1$.

If $\overline{e_2} \equiv_4 3$ and $\overline{e_3} \equiv_4 1$, then the only contributing terms in the second row are those involving R_1, $T_{1,5}$ and $T_{3,5}$. The product of the second row by $f((b_1,b_2))^t$ gives

$$\omega_{1_2} + \sum_{\substack{1\leq j\leq m_1\\ j\neq 2}} \chi_{\{3,7\}}(q_{1_j})\omega_{1_j} + \sum_{1\leq j\leq m_3} \chi_{\{3,7\}}(q_{3_j})\omega_{3_j}$$

which is equal to 0 if and only if $(-1)^{v_2(b_1)}\overline{b_1} \equiv_4 1$.

If $\overline{e_2} \equiv_4 3$ and $\overline{e_3} \equiv_4 3$, then the only contributing terms in the second row are those involving $T_{2,5}$ and $T_{3,5}$. The product of the second row by $f((b_1,b_2))^t$ gives

$$\sum_{\substack{1\leq j\leq m_2\\ j\neq 2}} \chi_{\{3,7\}}(q_{2_j})\omega_{2_j} + \sum_{1\leq j\leq m_3} \chi_{\{3,7\}}(q_{3_j})\omega_{3_j}$$

which is equal to 0 if and only if $\overline{b_2} \equiv_4 1$.

In sum, the second row represents the second condition appearing in each cell of the $v_2(e_2) = 1$ column of the table of Theorem 3.3.1.

The content of the third row depends on the values of $\overline{e_2}$ modulo 4 and $\overline{e_3}$ modulo 8. As in the second row, the difference between the cases is represented using the function χ. In the following subcases, we remark that since the primes q_{3_j} either divide both b_1 and b_2 or neither, the primes q_{3_j} always appear an even number of times when studying b_1b_2. Because the exponent of the primes divisors of b_1b_2 are in $\mathbb{Z}/2\mathbb{Z}$, the primes q_{3_j} can be ignored.

If $\overline{e_2} \equiv_4 1$ and $\overline{e_3} \equiv_8 1$, then the only contributing terms in the third row are those involving $T_{1,7}$ and $T_{2,7}$. The product of the third row by $f((b_1,b_2))^t$ gives

$$\sum_{\substack{1\leq j\leq m_1\\ j\neq 2}} \chi_{\{3,5\}}(q_{1_j})\omega_{1_j} + \sum_{\substack{1\leq j\leq m_2\\ j\neq 2}} \chi_{\{3,5\}}(q_{2_j})\omega_{2_j}.$$

This number collects the sum of exponents corresponding to the prime factors of $\overline{b_1b_2}$ that are congruent to 3 or 5 modulo 8. This sum is equal to 0 if and only if $\overline{b_1b_2} \equiv_8 1$ or 7.

If $\overline{e_2} \equiv_4 1$ and $\overline{e_3} \equiv_8 5$, then the only contributing terms in the third row are those involving R_1, $T_{1,7}$ and $T_{2,7}$. The product of the third row by $f((b_1,b_2))^t$ gives

$$\omega_{1_2} + \sum_{\substack{1\le j\le m_1\\ j\ne 2}} \chi_{\{3,5\}}(q_{1_j})\omega_{1_j} + \sum_{\substack{1\le j\le m_2\\ j\ne 2}} \chi_{\{3,5\}}(q_{2_j})\omega_{2_j}.$$

This number collects the sum of the exponents corresponding to the prime factors of $\overline{b_1b_2}$ that are congruent to 3 or 5 modulo 8 and the 2-valuation of b_1. This sum is equal to 0 if and only if $3^{v_2(b_1)}\overline{b_1b_2} \equiv_8 1$ or 7. When $2 \nmid b_1$, the row represents the condition $\overline{b_1b_2} \equiv_8 1$ or 7. When $2 \mid b_1$, the row represents the condition $3\overline{b_1b_2} \equiv_8 1$ or 7.

If $\overline{e_2} \equiv_4 1$ and $\overline{e_3} \equiv_8 3$, then the only contributing terms in the third row are those involving R_1, $T_{1,3}$ and $T_{2,3}$. The product of the third row by $f((b_1,b_2))^t$ gives

$$\omega_{1_2} + \sum_{\substack{1\le j\le m_1\\ j\ne 2}} \chi_{\{5,7\}}(q_{1_j})\omega_{1_j} + \sum_{\substack{1\le j\le m_2\\ j\ne 2}} \chi_{\{5,7\}}(q_{2_j})\omega_{2_j}.$$

This number collects the sum of the exponents corresponding to the prime factors of $\overline{b_1b_2}$ that are congruent to 5 or 7 modulo 8 and the 2-valuation of b_1. This sum is equal to 0 if and only if $(-1)^{v_2(b_1)}\overline{b_1b_2} \equiv_8 1$ or 3. When $2 \nmid b_1$, the row represents the condition $\overline{b_1b_2} \equiv_8 1$ or 3. When $2 \mid b_1$, the row represents the condition $-\overline{b_1b_2} \equiv_8 1$ or 3.

If $\overline{e_2} \equiv_4 1$ and $\overline{e_3} \equiv_8 7$, then the only contributing terms in the third row are those involving $T_{1,3}$ and $T_{2,3}$. The product of the third row by $f((b_1,b_2))^t$ gives

$$\sum_{\substack{1\le j\le m_1\\ j\ne 2}} \chi_{\{5,7\}}(q_{1_j})\omega_{1_j} + \sum_{\substack{1\le j\le m_2\\ j\ne 2}} \chi_{\{5,7\}}(q_{2_j})\omega_{2_j}$$

This number collects the sum of exponents corresponding to the prime factors of $\overline{b_1b_2}$ that are congruent to 5 or 7 modulo 8. This sum is equal to 0 if and only if $\overline{b_1b_2} \equiv_8 1$ or 3.

If $\overline{e_2} \equiv_4 3$ and $\overline{e_3} \equiv_8 1$, then the only contributing terms in the third row are those involving R_1, $T_{1,3}$ and $T_{2,3}$. The product of the third row by $f((b_1,b_2))^t$ gives

$$\omega_{1_2} + \sum_{\substack{1\le j\le m_1\\ j\ne 2}} \chi_{\{5,7\}}(q_{1_j})\omega_{1_j} + \sum_{\substack{1\le j\le m_2\\ j\ne 2}} \chi_{\{5,7\}}(q_{2_j})\omega_{2_j}$$

which is equal to 0 if and only if $(-1)^{v_2(b_1)}\overline{b_1b_2} \equiv_8 1$ or 3.

If $\overline{e_2} \equiv_4 3$ and $\overline{e_3} \equiv_8 5$, then the only contributing terms in the third row are those involving $T_{1,3}$ and $T_{2,3}$. The product of the third row by $f((b_1,b_2))^t$ gives

$$\sum_{\substack{1\leq j\leq m_1\\ j\neq 2}} \chi_{\{5,7\}}(q_{1_j})\omega_{1_j} + \sum_{\substack{1\leq j\leq m_2\\ j\neq 2}} \chi_{\{5,7\}}(q_{2_j})\omega_{2_j}$$

which is equal to 0 if and only if $\overline{b_1 b_2} \equiv_8 1$ or 3.

If $\overline{e_2} \equiv_4 3$ and $\overline{e_3} \equiv_8 3$, then the only contributing terms in the third row are those involving R_1, $T_{1,7}$ and $T_{2,7}$. The product of the third row by $f((b_1,b_2))^t$ gives

$$\omega_{1_2} + \sum_{\substack{1\leq j\leq m_1\\ j\neq 2}} \chi_{\{3,5\}}(q_{1_j})\omega_{1_j} + \sum_{\substack{1\leq j\leq m_2\\ j\neq 2}} \chi_{\{3,5\}}(q_{2_j})\omega_{2_j}$$

which is equal to 0 if and only if $3^{v_2(b_1)}\overline{b_1 b_2} \equiv_8 1$ or 7.

If $\overline{e_2} \equiv_4 3$ and $\overline{e_3} \equiv_8 7$, then the only contributing terms in the third row are those involving $T_{1,7}$ and $T_{2,7}$. The product of the third row by $f((b_1,b_2))^t$ gives

$$\sum_{\substack{1\leq j\leq m_1\\ j\neq 2}} \chi_{\{3,5\}}(q_{1_j})\omega_{1_j} + \sum_{\substack{1\leq j\leq m_2\\ j\neq 2}} \chi_{\{3,5\}}(q_{2_j})\omega_{2_j}$$

which is equal to 0 if and only if $\overline{b_1 b_2} \equiv_8 1$ or 7.

In sum, the third row represents the third condition appearing in each cell of the $v_2(e_2) = 1$ column of the table of Theorem 3.3.1.

□

Here we record the matrices corresponding to the remaining columns in the tables from Theorems 3.3.1, 3.3.2, 3.3.3 and 3.3.4.

Lemma 4.3.6. *If $2 \nmid e_3$ and $v_2(e_2) = 2$, we have that*

$$M_{\mathbb{Q}_2} = \left(\begin{array}{c|c|c} R_1 & O_{1,m_3} & R_2 \\ \hline \begin{matrix}(1+\chi_{\{3,7\}}(e_2)\chi_{\{1,5\}}(e_3))T_{1,5}\\ +R_1\end{matrix} & \chi_{\{1,5\}}(e_3)T_{3,5} & (1+\chi_{\{1,5\}}(e_2)\chi_{\{1,5\}}(e_3))T_{1,5} \\ \hline \begin{matrix}\chi_{\{1,5\}}(e_2)\chi_{\{3\}}(e_3)T_{1,7}\\ +\chi_{\{3,7\}}(e_2)\chi_{\{7\}}(e_3)T_{1,7}\\ +R_1\end{matrix} & \begin{matrix}\chi_{\{1,5\}}(e_2)\chi_{\{3\}}(e_3)T_{3,5}\\ +\chi_{\{3,7\}}(e_2)\chi_{\{7\}}(e_3)T_{3,5}\end{matrix} & \begin{matrix}\chi_{\{1,5\}}(e_2)\chi_{\{3\}}(e_3)T_{2,3}\\ +\chi_{\{3,7\}}(e_2)\chi_{\{7\}}(e_3)T_{2,3}\end{matrix} \end{array}\right).$$

Lemmas 4.3.5 and 4.3.6 codify the statement of Theorem 3.3.1.

Lemma 4.3.7. *If* $2 \nmid e_3$ *and* $v_2(e_2) = 3$*, we have that*

$$M_{\mathbb{Q}_2} = \left(\begin{array}{c|c|c} R_1 & O_{1,m_3} & R_2 \\ \hline \begin{array}{c} \chi_{\{1,5\}}(e_2)\chi_{\{3,5,7\}}(e_3)T_{1,5} \\ +\chi_{\{3,7\}}(e_2)\chi_{\{1,5,7\}}(e_3)T_{1,5} \\ +\chi_{\{1\}}(e_3)R_1 \end{array} & \chi_{\{1,5\}}(e_2)T_{3,5} & \begin{array}{c} \chi_{\{1,5\}}(e_2)\chi_{\{1,3,7\}}(e_3)T_{2,5} \\ +\chi_{\{3,7\}}(e_2)\chi_{\{3,5,7\}}(e_3)T_{2,5} \end{array} \\ \hline \begin{array}{c} \chi_{\{1,3\}}(e_3)T_{1,3} \\ +\chi_{\{5,7\}}(e_3)T_{1,7} \\ +\chi_{\{1,3,5\}}(e_3)R_1 \end{array} & O_{1,m_3} & \begin{array}{c} \chi_{\{1,3\}}(e_3)T_{2,3} \\ +\chi_{\{5,7\}}(e_3)T_{2,7} \end{array} \end{array}\right).$$

Lemma 4.3.8. *If* $2 \nmid e_3$ *and* $v_2(e_2) = 4$*, we have that*

$$M_{\mathbb{Q}_2} = \left(\begin{array}{c|c|c} R_1 & O_{1,m_3} & R_2 \\ \hline \begin{array}{c} (1+\chi_{\{3,7\}}(e_2)\chi_{\{1,5\}}(e_3))T_{1,5} \\ +\chi_{\{5\}}(e_3)R_1 \end{array} & \chi_{\{1,5\}}(e_3)T_{3,5} & (1+\chi_{\{1,5\}}(e_2)\chi_{\{1,5\}}(e_3))T_{2,5} \\ \hline \begin{array}{c} \chi_{\{1\}}(e_3)T_{1,7} \\ +\chi_{\{5\}}(e_3)T_{1,3} \\ +\chi_{\{3,7\}}(e_3)R_1 \end{array} & O_{1,m_3} & \begin{array}{c} \chi_{\{1\}}(e_3)T_{2,7} \\ +\chi_{\{5\}}(e_3)T_{2,3} \end{array} \end{array}\right).$$

Lemmas 4.3.7 and 4.3.8 codify the statement of Theorem 3.3.2.

Lemma 4.3.9. *If* $2 \nmid e_3$*,* $32 \mid e_2$ *and* $v_2(e_2) \equiv_2 1$*, we have that*

$$M_{\mathbb{Q}_2} = \left(\begin{array}{c|c|c} R_1 & O_{1,m_3} & R_2 \\ \hline \begin{array}{c} \chi_{\{1,5\}}(e_2)\chi_{\{1,3,7\}}(e_3)T_{1,5} \\ +\chi_{\{3,7\}}(e_2)\chi_{\{3,5,7\}}(e_3)T_{1,5} \\ +\chi_{\{5\}}(e_3)R_1 \end{array} & \chi_{\{1,5\}}(e_3)T_{3,5} & \begin{array}{c} \chi_{\{1,5\}}(e_2)\chi_{\{3,5,7\}}(e_3)T_{2,5} \\ +\chi_{\{3,7\}}(e_2)\chi_{\{1,3,7\}}(e_3)T_{1,5} \end{array} \\ \hline \begin{array}{c} \chi_{\{1,3\}}(e_3)T_{1,7} \\ +\chi_{\{5,7\}}(e_3)T_{1,3} \\ +\chi_{\{5\}}R_1 \end{array} & O_{1,m_3} & \begin{array}{c} \chi_{\{1,3\}}(e_3)T_{2,7} \\ +\chi_{\{5,7\}}(e_3)T_{2,3} \end{array} \end{array}\right).$$

Lemma 4.3.10. *If* $2 \nmid e_3$*,* $32 \mid e_2$ *and* $v_2(e_2) \equiv_2 0$*, we have that*

$$M_{\mathbb{Q}_2} = \left(\begin{array}{c|c|c} R_1 & O_{1,m_3} & R_2 \\ \hline \begin{array}{c} (1+\chi_{\{3,7\}}(e_2)\chi_{\{1,5\}}(e_3))T_{1,5} \\ +\chi_{\{5\}}(e_3)R_1 \end{array} & \chi_{\{1,5\}}(e_3)T_{3,5} & (1+\chi_{\{1,5\}}(e_2)\chi_{\{1,5\}}(e_3))T_{2,5} \\ \hline \begin{array}{c} \chi_{\{1\}}(e_3)T_{1,7} \\ +\chi_{\{5,7\}}(e_3)T_{1,3} \\ +\chi_{\{3\}}(e_3)R_1 \end{array} & O_{1,m_3} & \begin{array}{c} \chi_{\{1\}}(e_3)T_{2,7} \\ +\chi_{\{5,7\}}(e_3)T_{2,3} \end{array} \end{array}\right).$$

Lemmas 4.3.9 and 4.3.10 codify the statement of Theorem 3.3.3.

Lemma 4.3.11. *If* $2 \mid e_3$, $v_2(e_2) = 2$ *and* $\overline{e_3} \equiv_4 1$, *we have that*

$$M_{\mathbb{Q}_2} = \left(\begin{array}{c|c|c} T_{1,7}+\chi_{\{3,5\}}(e_2e_3)R_1 & T_{3,7} & \chi_{\{3,5\}}(e_2)R_2 \\ \hline \chi_{\{5,7\}}(-e_2)R_1 & T_{3,3} & T_{2,3}+\chi_{\{5,7\}}(-e_2(e_3-e_2))R_2 \\ \hline T_{1,5}+R_1 & O_{1,m_3} & T_{2,5} \end{array}\right).$$

Lemma 4.3.12. *If* $2 \mid e_3$, $v_2(e_2) = 2$ *and* $\overline{e_3} \equiv_4 3$, *we have that*

$$M_{\mathbb{Q}_2} = \left(\begin{array}{c|c|c} T_{1,3}+\chi_{\{5,7\}}(e_2e_3)R_1 & T_{3,3} & \chi_{\{5,7\}}(e_2)R_2 \\ \hline \chi_{\{3,5\}}(e_2)R_1 & T_{3,7} & T_{2,7}+\chi_{\{3,5\}}(e_2(e_3-e_2))R_2 \\ \hline T_{1,5} & O_{1,m_3} & T_{2,5}+R_2 \end{array}\right).$$

Lemma 4.3.13. *If* $2 \mid e_3$, $v_2(e_2) = 3$ *and* $\overline{e_3} \equiv_4 1$, *we have that*

$$M_{\mathbb{Q}_2} = \left(\begin{array}{c|c|c} T_{1,3}+\chi_{\{5,7\}}(e_2)R_1 & T_{3,3} & \chi_{\{5,7\}}(e_2e_3)R_2 \\ \hline \chi_{\{5,7\}}(e_2e_3)R_1 & T_{3,3} & T_{2,3}+\chi_{\{5,7\}}(-e_2)R_2 \\ \hline T_{1,5}+R_1 & O_{1,m_3} & T_{2,5}+R_2 \end{array}\right).$$

Lemma 4.3.14. *If* $2 \mid e_3$, $v_2(e_2) = 3$ *and* $\overline{e_3} \equiv_4 3$, *we have that*

$$M_{\mathbb{Q}_2} = \left(\begin{array}{c|c|c} T_{1,7}+\chi_{\{3,5\}}(e_2)R_1 & T_{3,7} & \chi_{\{3,5\}}(e_2e_3)R_2 \\ \hline \chi_{\{3,5\}}(3e_2e_3)R_1 & T_{3,7} & T_{2,7}+\chi_{\{3,5\}}(e_2)R_2 \\ \hline T_{1,5} & O_{1,m_3} & T_{2,5} \end{array}\right).$$

Lemma 4.3.15. *If* $2 \mid e_3$, $16 \mid e_2$, $v_2(e_2) \equiv_2 0$ *and* $\overline{e_3} \equiv_4 1$, *we have that*

$$M_{\mathbb{Q}_2} = \left(\begin{array}{c|c|c} T_{1,3} + \chi_{\{5,7\}}(e_2e_3)R_1 & T_{3,3} & \chi_{\{5,7\}}(e_2)R_2 \\ \hline \chi_{\{5,7\}}(-e_2)R_1 & T_{3,3} & T_{2,3} + \chi_{\{5,7\}}(-e_2e_3)R_2 \\ \hline T_{1,5} + R_1 & O_{1,m_3} & T_{2,5} + R_2 \end{array}\right).$$

Lemma 4.3.16. *If* $2 \mid e_3$, $16 \mid e_2$, $v_2(e_2) \equiv_2 0$ *and* $\overline{e_3} \equiv_4 3$, *we have that*

$$M_{\mathbb{Q}_2} = \left(\begin{array}{c|c|c} T_{1,7} + \chi_{\{3,5\}}(e_2e_3)R_1 & T_{3,7} & \chi_{\{3,5\}}(e_2)R_2 \\ \hline \chi_{\{3,5\}}(e_2)R_1 & T_{3,7} & T_{2,7} + \chi_{\{3,5\}}(e_2e_3)R_2 \\ \hline T_{1,5} & O_{1,m_3} & T_{2,5} \end{array}\right).$$

Lemma 4.3.17. *If* $2 \mid e_3$, $16 \mid e_2$, $v_2(e_2) \equiv_2 1$ *and* $\overline{e_3} \equiv_4 1$, *we have that*

$$M_{\mathbb{Q}_2} = \left(\begin{array}{c|c|c} T_{1,3} + \chi_{\{5,7\}}(e_2)R_1 & T_{3,3} & \chi_{\{5,7\}}(e_2e_3)R_2 \\ \hline \chi_{\{5,7\}}(-e_2e_3)R_1 & T_{3,3} & T_{2,3} + \chi_{\{5,7\}}(-e_2)R_2 \\ \hline T_{1,5} + R_1 & O_{1,m_3} & T_{2,5} + R_2 \end{array}\right).$$

Lemma 4.3.18. *If* $2 \mid e_3$, $16 \mid e_2$, $v_2(e_2) \equiv_2 1$ *and* $\overline{e_3} \equiv_4 3$, *we have that*

$$M_{\mathbb{Q}_2} = \left(\begin{array}{c|c|c} T_{1,7} + \chi_{\{3,5\}}(e_2)R_1 & T_{3,7} & \chi_{\{3,5\}}(e_2e_3)R_2 \\ \hline \chi_{\{3,5\}}(e_2e_3)R_1 & T_{3,7} & T_{2,7} + \chi_{\{3,5\}}(e_2)R_2 \\ \hline T_{1,5} & O_{1,m_3} & T_{2,5} \end{array}\right).$$

Lemmas 4.3.11 to 4.3.18 codify the statement of Theorem 3.3.4.

4.4. Matrix rows for $\mathbb{Q}_p$

When e_2 and e_3 are fixed and p is an odd prime number dividing δ, there are two conditions for a solution in $\mathbb{Q}_p$.

When $p \mid GCD(e_2,e_3)$, we will need two matrix rows.

When $p \nmid GCD(e_2,e_3)$, one of the conditions is already represented in the subgroup H of $\mathbb{Q}(S,2) \times \mathbb{Q}(S,2)$. We will then only need one matrix row.

We will call $M_{\mathbb{Q}_{p,1}}$ the sub-matrix representing all the conditions for the primes not dividing $GCD(e_2,e_3)$ and $M_{\mathbb{Q}_{p,2}}$ the sub-matrix representing all the conditions for the primes dividing $GCD(e_2,e_3)$.

As in the preceding case, we start by defining the building blocks that will be needed to construct the submatrices.

Definition 4.4.1. *For p an odd prime and $i \in \{1,2,3\}$, we define $W_{i,p}$ as:*

$$W_{i,p} = (w_{1,k}) \text{ for } 1 \leq k \leq m_i,$$
$$w_{1,k} = \begin{cases} 1 \text{ if } q_{i_k} = p, \\ 0 \text{ otherwise.} \end{cases}$$

The role of $W_{1,p}$ is to check if $p \mid b_1$, the role of $W_{2,p}$ is to check if $p \mid b_2$ and the role of $W_{3,p}$ is to check if $p \mid b_1$ and $p \mid b_2$ simultaneously.

Definition 4.4.2. *For p an odd prime and $i \in \{1,2,3\}$, we define $V_{i,p}$ as:*

$$V_{i,p} = (v_{1,k}) \text{ for } 1 \leq k \leq m_i,$$
$$v_{1,k} = \begin{cases} 1 \text{ if } \left(\dfrac{q_{i_k}}{p}\right) = -1, \\ 0 \text{ otherwise.} \end{cases}$$

When combined, the roles of $V_{i,p}$ (for $i \in \{1,2\}$) and $V_{3,p}$ are to check the value of $\left(\frac{\overline{b_i}}{p}\right)$.

Remark here that we require that $\left(\frac{q_{i_k}}{p}\right) = -1$, this means that $w_{1,k} = 0$ if $q_{i_k} = p$.

As in the case of $\mathbb{Q}_2$ we will also need a function that will act as an indicator function:

Definition 4.4.3. *Let p be a prime number and a be an integer with $\overline{a} = \frac{a}{p^{v_p(a)}}$, we define the function h_p as:*

$$h_p(a) = \begin{cases} 1 \text{ if } \left(\dfrac{\overline{a}}{p}\right) = -1, \\ 0 \text{ otherwise.} \end{cases}$$

4.4.1. Matrix rows when $p \nmid GCD(e_2,e_3)$

We shall denote by N_p the matrix row representing the conditions in $\mathbb{Q}_p$.

Lemma 4.4.4. *Let $p \mid e_2$ and $p \nmid e_3$.*

If $v_p(e_2) \equiv_2 1$, we have that

$$N_p = \left(\begin{array}{c|c|c} V_{1,p} & W_{3,p} & V_{2,p} \end{array} \right).$$

If $v_p(e_2) \equiv_2 0$, we have that

$$N_p = \left(\; (1+h_p(-e_3))V_{1,p} \;\middle|\; h_p(-e_3)W_{3,p} \;\middle|\; (1+h_p(-e_3))V_{2,p} \; \right).$$

Lemma 4.4.5. *Let $p \nmid e_2$ and $p \mid e_3$.*

If $v_p(e_3) \equiv_2 1$, we have that

$$N_p = \left(\; W_{1,p} \;\middle|\; V_{3,p} \;\middle|\; V_{2,p} \; \right).$$

If $v_p(e_3) \equiv_2 0$, we have that

$$N_p = \left(\; h_p(-e_2)W_{1,p} \;\middle|\; (1+h_p(-e_2))V_{3,p} \;\middle|\; (1+h_p(-e_2))V_{2,p} \; \right).$$

Lemma 4.4.6. *Let $p \nmid e_2$ and $p \mid e_3 - e_2$.*

If $v_p(e_3 - e_2) \equiv_2 1$, we have that

$$N_p = \left(\; V_{1,p} \;\middle|\; V_{3,p} \;\middle|\; W_{2,p} \; \right).$$

If $v_p(e_3 - e_2) \equiv_2 0$, we have that

$$N_p = \left(\; (1+h_p(e_3))V_{1,p} \;\middle|\; (1+h_p(e_3))V_{3,p} \;\middle|\; h_p(e_3)W_{2,p} \; \right).$$

Lemmas 4.4.4, 4.4.5 and 4.4.6 codify the statement of Theorem 3.4.1.

We can now have the following corollary:

Lemma 4.4.7. *With the above matrix rows, we can define $M_{\mathbb{Q}_p,1}$ as:*

$$M_{\mathbb{Q}_p,1} = \left(\begin{array}{c} N_{p_{5_1}} \\ \vdots \\ N_{p_{5_{n_5}}} \\ \hline N_{p_{6_1}} \\ \vdots \\ N_{p_{6_{n_6}}} \\ \hline N_{p_{7_1}} \\ \vdots \\ N_{p_{7_{n_7}}} \end{array} \right).$$

4.4.2. Matrix rows when $p \mid GCD(e_2,e_3)$

When $p \mid GCD(e_2,e_3)$, we have two matrix rows. The first one, that we will call $N_{p,1}$, represents a condition on b_1. The other row, that we will call $N_{p,2}$, represents a condition on b_2.

We will use the same building blocks as in the preceding subsection.

Lemma 4.4.8. *If $p^3 \mid\mid e_2e_3(e_3-e_2)$, we have that:*

$$N_{p,1} = \left(\; V_{1,p} + h_p(e_2)W_{1,p} \; \middle| \; V_{3,p} \; \middle| \; h_p(e_2e_3)W_{2,p} \; \right),$$
$$N_{p,2} = \left(\; h_p(-e_2(e_3-e_2))W_{1,p} \; \middle| \; V_{3,p} \; \middle| \; V_{2,p} + h_p(-e_2)W_{2,p} \; \right).$$

Lemma 4.4.9. *Let $p^2 \mid e_2$.*

If $v_p(e_2) \equiv_2 0$, we have that:

$$N_{p,1} = \left(\; V_{1,p} + h_p(e_2e_3)W_{1,p} \; \middle| \; V_{3,p} \; \middle| \; h_p(e_2)W_{2,p} \; \right),$$
$$N_{p,2} = \left(\; h_p(-e_2)W_{1,p} \; \middle| \; V_{3,p} \; \middle| \; V_{2,p} + h_p(-e_2e_3)W_{2,p} \; \right).$$

If $v_p(e_2) \equiv_2 1$, we have that:

$$N_{p,1} = \left(\; V_{1,p} + h_p(e_2)W_{1,p} \; \middle| \; V_{3,p} \; \middle| \; h_p(e_2e_3)W_{2,p} \; \right),$$
$$N_{p,2} = \left(\; h_p(-e_2e_3)W_{1,p} \; \middle| \; V_{3,p} \; \middle| \; V_{2,p} + h_p(-e_2)W_{2,p} \; \right).$$

Lemma 4.4.10. *Let $p^2 \mid e_3$.*

If $v_p(e_3) \equiv_2 0$, we have that:

$$N_{p,1} = \left(\; V_{1,p} + h_p(e_2)W_{1,p} \; \middle| \; V_{3,p} \; \middle| \; h_p(e_3)W_{2,p} \; \right),$$
$$N_{p,2} = \left(\; O_{1,m_1} \; \middle| \; V_{3,p} \; \middle| \; V_{2,p} + h_p(-e_2)W_{2,p} \; \right).$$

If $v_p(e_3) \equiv_2 1$, we have that:

$$N_{p,1} = \left(\; V_{1,p} + h_p(e_2)W_{1,p} \; \middle| \; V_{3,p} \; \middle| \; h_p(e_2e_3)W_{2,p} \; \right),$$
$$N_{p,2} = \left(\; O_{1,m_1} \; \middle| \; V_{3,p} \; \middle| \; V_{2,p} + h_p(-e_2)W_{2,p} \; \right).$$

Lemma 4.4.11. *Let $p \mid e_3 - e_2$.*

If $v_p(e_3-e_2) \equiv_2 0$, we have that:

$$N_{p,1} = \left(\; V_{1,p} + h_p(e_2)W_{1,p} \; \middle| \; V_{3,p} \; \middle| \; O_{1,m_2} \; \right),$$
$$N_{p,2} = \left(\; h_p(e_3 - e_2)W_{1,p} \; \middle| \; V_{3,p} \; \middle| \; V_{2,p} + h_p(-e_2)W_{2,p} \; \right).$$

If $v_p(e_3 - e_2) \equiv_2 1$, we have that:

$$N_{p,1} = \left(\; V_{1,p} + h_p(e_2)W_{1,p} \; \middle| \; V_{3,p} \; \middle| \; O_{1,m_2} \; \right),$$
$$N_{p,2} = \left(\; h_p(-e_2(e_3 - e_2))W_{1,p} \; \middle| \; V_{3,p} \; \middle| \; V_{2,p} + h_p(-e_2)W_{2,p} \; \right).$$

Lemmas 4.4.8 to 4.4.11 codify the statement of Theorem 3.4.2.

We now have the following corollary:

Lemma 4.4.12. *With the above matrix rows, if we write $m = 2 + n_1 + n_2 + n_3 + n_4$, we can define $M_{\mathbb{Q}_p,2}$ as:*

$$M_{\mathbb{Q}_p,2} = \left(\begin{array}{c} N_{q_{1_3},1} \\ \vdots \\ N_{q_{1_m},1} \\ \hline N_{q_{1_3},2} \\ \vdots \\ N_{q_{1_m},2} \end{array} \right).$$

The rows are organized so that the upper half contains the conditions for b_1 and the second half contains the conditions for b_2. We do this so that it is easier to work with the matrix later.

4.5. Construction of the matrix

Now that we have determined the rows for a local solution for each p-adic set, we can put them together to get:

Theorem 4.5.1. *Let $E(\mathbb{Q}) : y^2 = x(x - e_2)(x - e_3)$ be an elliptic curve with e_2,e_3 respecting the conditions of Section 3.1. Also, let:*

$$M_{e_2,e_3} = \left(\begin{array}{c} M_{\mathbb{R}} \\ \hline M_{\mathbb{Q}_2} \\ \hline M_{\mathbb{Q}_{p,1}} \\ \hline M_{\mathbb{Q}_{p,2}} \end{array} \right).$$

We then have that:

$$\dim(\ker(M_{e_2,e_3})) = \operatorname{rank}(Sel_2(E(\mathbb{Q}))) - 2.$$

PROOF. Since M_{e_3,e_2} is the superposition of the matrices verifying each of the local conditions, its kernel is bijective to the set of $(b_1{,}b_2)$ respecting every local condition. □

This gives us the central corollary of this work:

Corollary 4.5.2. *Let* $E(\mathbb{Q}) : y^2 = x(x-e_2)(x-e_3)$ *be an elliptic curve with* $e_2{,}e_3$ *respecting the conditions of Section 3.1. If* $\dim(\ker(M_{e_2,e_3})) = 2$*, then the rank of* $E(\mathbb{Q})$ *is 0.*

Chapter 5

Applications of the Generalized Monsky Matrix

5.1. Generalized induction theorem

Now that we have constructed the Generalized Monsky Matrix, we proceed to extract results from it.

In [**Mok20**], we showed what we called induction theorems in elliptic curves of the $\frac{\pi}{3}$ and $\frac{2\pi}{3}$-congruent number problems. The idea is that if n is non θ-congruent, then, when respecting certain conditions, we can find two distinct primes p and q such that pqn is also non-θ-congruent.

In this section, we give a similar theorem that will apply to most elliptic curves in Legendre form.

Before doing anything else, we start with two definitions that will simplify the notation.

Definition 5.1.1. *We define* $K(e_2,e_3) := \dim \ker M_{e_2,e_3}$.

Definition 5.1.2. *Let* $A_{m_A \times n_A}$ *and* $B_{m_B \times n_B}$ *be two matrices, we define the equivalence relation:*

$$A \sim B \iff m_A - rank(A) = m_B - rank(B).$$

In other words, A and B are equivalent if an only if their echelon form have the same number of null rows.

We will use the following lemma to work with the equivalence relation.

Lemma 5.1.3. *There are some basic operations from linear algebra that keep the equivalent relation of Definition 5.1.2:*

(1) Adding a row to another.

(2) Removing a row that is linearly independent from the others.

(3) Removing a column that only contains zeros.

We are interested in this relation because of the following result whose proof is immediate:

Proposition 5.1.4. *Let A and B be two square matrices. We have that*

$$A \sim B \iff \dim\ker A = \dim\ker B.$$

Since the Generalized Monsky Matrix is always square, we have that $K(e_2,e_3) = K(e_2',e_3')$ if and only if $M_{e_2,e_3} \sim M_{e_2',e_3'}$.

The goal here is, for a given pair (e_2,e_3), to find two primes $p,q \nmid e_2e_3(e_3-e_2)$ such that $K(pqe_2,pqe_3) = K(e_2,e_3)$ by showing that $M_{pqe_2,pqe_3} \sim M_{e_2,e_3}$.

In order to do this, we construct what call the induction submatrix:

Definition 5.1.5. *Let e_2 and e_3 be two integers respecting the conditions of Section 3.1 and let p,q be two distinct prime numbers such that $p,q \nmid e_2e_3(e_3-e_2)$. We define the induction submatrix $H_{e_2,e_3,p,q}$ as:*

$$H_{e_2,e_3,p,q} := \left(\begin{array}{cc|cc} h_p(qe_2) & h_p(q) & h_p(e_2e_3) & 0 \\ h_q(p) & h_q(pe_2) & 0 & h_q(e_2e_3) \\ \hline h_p(-e_2(e_3-e_2)) & 0 & h_p(-qe_2) & h_p(q) \\ 0 & h_q(-e_2(e_3-e_2)) & h_q(p) & h_q(-pe_2) \end{array}\right),$$

where the coefficients are given by Definition 4.4.3.

The reason it is called induction submatrix will become clear in Theorem 5.1.8. We need to introduce some new notation before stating the theorem.

We first want to separate $H_{e_2,e_3,p,q}$ in four parts:

Definition 5.1.6.

$$\begin{cases} H_1 := \begin{pmatrix} h_p(qe_2) & h_p(q) \\ h_q(p) & h_q(pe_2) \end{pmatrix}, \\ H_2 := \begin{pmatrix} h_p(e_2e_3) & 0 \\ 0 & h_q(e_2e_3) \end{pmatrix}, \\ H_3 := \begin{pmatrix} h_p(-e_2(e_3-e_2)) & 0 \\ 0 & h_q(-e_2(e_3-e_2)) \end{pmatrix}, \\ H_4 := \begin{pmatrix} h_p(-qe_2) & h_p(q) \\ h_q(p) & h_q(-pe_2) \end{pmatrix}. \end{cases}$$

Thus we can write

$$H_{e_2,e_3,p,q} := \left(\begin{array}{c|c} H_1 & H_2 \\ \hline H_3 & H_4 \end{array}\right).$$

We also introduce the following notation:

Definition 5.1.7. *We call J_i the ith row of $H_{e_2,e_3,p,q}$.*

This notation will be useful for the proof of Theorem 5.1.8 when we combine it with the notation that comes next. We introduce the least intuitive notation. We separate M_{e_2,e_3} in nine submatrices. This will be clearer when we apply the notation later in Theorem 5.1.8. More precisely, we write:

$$M_{e_2,e_3} = \left(\begin{array}{c|c|c} M_1 & M_2 & M_3 \\ \hline M_4 & M_5 & M_6 \\ \hline M_7 & M_8 & M_9 \end{array}\right),$$

with M_1 being of dimension $(4+\sum_{i=5}^7 n_i)\times(2)$, M_2 being of dimension $(4+\sum_{i=5}^7 n_i)\times(m_1+m_3)$, M_3 being of dimension $(4+\sum_{i=5}^7 n_i)\times(m_2-2)$, M_4 being of dimension $(\sum_{i=1}^4 n_i)\times(2)$, M_5 being of dimension $(\sum_{i=1}^4 n_i)\times(m_1+m_3)$, M_6 being of dimension $(\sum_{i=1}^4 n_i)\times(m_2-2)$, M_7 being of dimension $(\sum_{i=1}^4 n_i)\times(2)$, M_8 being of dimension $(\sum_{i=1}^4 n_i)\times(m_1+m_3)$ and M_9 being of dimension $(\sum_{i=1}^4 n_i)\times(m_2-2)$.

Here is an intuitive way to see the new decomposition. Multiplication of e_2 and e_3 by pq corresponds to adding 4 new columns and lines. By looking at the positions of these new columns and lines, one can remark that they are grouped in pairs. Using each of these pairs as a border separates the rest of the matrix in 9 parts. Those 9 parts are our 9 submatrices.

Finally, we write C_s to represent any $n \times 2$ sub-matrix (the size of n is defined by the context) such that $c_{i,1} = c_{i,2}$. Similarly, we write L_s to represent any $2 \times n$ sub-matrix (the size of n is not necessarily the same as the ones before) such that $l_{1,j} = l_{2,j}$. They can be seen as two equal vectors, but next to each other.

With all the previous notation introduced, we can state the following theorem.

Theorem 5.1.8. *Let e_2 and e_3 be two integers respecting the conditions of Section 3.1. Let p and q be two distinct prime numbers such that:*

$$\begin{cases} p,q \nmid e_2e_3(e_2 - e_3), \\ p \equiv_8 q, \\ \forall s \mid e_2e_3(e_2-e_3) \in \mathcal{P}\backslash\{2\}, \left(\dfrac{p}{s}\right) = \left(\dfrac{q}{s}\right), \\ \det\left(H_{e_2,e_3,p,q}\right) = 1, \\ \langle J_1 + J_2, J_3 + J_4 \rangle = \left\langle \begin{pmatrix} 1 & 1 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 1 & 1 \end{pmatrix} \right\rangle. \end{cases}$$

We then have that $K(e_2,e_3) = K(pqe_2,pqe_3)$.

Proof. We will prove this by showing that $M_{e_2,e_3} \sim M_{pqe_2,pqe_3}$. We start by remarking that

$$M_{pqe_2,pqe_3} = \left(\begin{array}{c|c|c|c|c} M_1 & C_1 & M_2 & C_2 & M_3 \\ \hline L_1 & H_1 & L_2 & H_2 & L_3 \\ \hline M_4 & C_3 & M_5 & C_4 & M_6 \\ \hline L_4 & H_3 & L_5 & H_4 & L_6 \\ \hline M_7 & C_5 & M_8 & C_6 & M_9 \end{array}\right).$$

From the last condition in the hypothesis, we remark that we can use the rows not containing any C_i to generate the following two rows:

$$\begin{cases} \left(\; O \;\middle|\; (1,1) \;\middle|\; O \;\middle|\; (0,0) \;\middle|\; O \; \right), \\ \left(\; O \;\middle|\; (0,0) \;\middle|\; O \;\middle|\; (1,1) \;\middle|\; O \; \right). \end{cases}$$

By adding these rows to the appropriate matrix rows, we get that

$$M_{pqe_2,pqe_3} \sim \left(\begin{array}{c|c|c|c|c} M_1 & O & M_2 & O & M_3 \\ \hline L_1 & H_1 & L_2 & H_2 & L_3 \\ \hline M_4 & O & M_5 & O & M_6 \\ \hline L_4 & H_3 & L_5 & H_4 & L_6 \\ \hline M_7 & O & M_8 & O & M_9 \end{array}\right).$$

Since $H_{e_2,e_3,p,q}$ is invertible, we have that the rows of:

$$\left(\begin{array}{c|c|c|c|c} L_1 & H_1 & L_2 & H_2 & L_3 \\ \hline L_4 & H_3 & L_5 & H_4 & L_6 \end{array}\right)$$

are linearly independent to each other and to the other rows of M_{pqe_2,pqe_3}. This implies that

$$M_{pqe_2,pqe_3} \sim \left(\begin{array}{c|c|c|c|c} M_1 & O & M_2 & O & M_3 \\ \hline M_4 & O & M_5 & O & M_6 \\ \hline M_7 & O & M_8 & O & M_9 \end{array}\right).$$

We can now simply erase the columns containing only zeros to get that

$$M_{pqe_2,pqe_3} \sim \left(\begin{array}{c|c|c} M_1 & M_2 & M_3 \\ \hline M_4 & M_5 & M_6 \\ \hline M_7 & M_8 & M_9 \end{array}\right) = M_{e_2,e_3}.$$

□

As a consequence, we obtain Theorem 1.0.3.

Theorem 5.1.9 (Originally Theorem 1.0.3)**.** *Let e_2, e_3 be two integers respecting the conditions of Section 3.1 and p,q be distinct prime numbers with the following conditions:*

$$\begin{cases} p,q \nmid e_2e_3(e_2-e_3), \\ p \equiv_8 q, \\ \forall s \mid e_2e_3(e_2-e_3) \in \mathcal{P}\backslash\{2\}, \left(\frac{p}{s}\right) = \left(\frac{q}{s}\right). \end{cases}$$

If, additionally, one of the following conditions is satisfied:

(1) $p \equiv_4 1$ *and at least two of* $\left\{\left(\frac{e_2}{p}\right), \left(\frac{e_3}{p}\right), \left(\frac{e_3-e_2}{p}\right)\right\}$ *are negative.*

(2) $p \equiv_4 3$, $\left(\frac{e_3}{p}\right) = -\left(\frac{e_2}{p}\right)$ *and* $\left(\frac{e_3}{p}\right) = -\left(\frac{e_3-e_2}{p}\right)$.

We then have that $K(pqe_2,pqe_3) = K(e_2,e_3)$.

Proof. One can check, using Python, for example, that these are the conditions for which the induction matrix respects the hypothesis of Theorem 5.1.8. □

One can ask if there is a similar result to Theorem 5.1.8 when $\det\left(H_{e_2,e_3,p,q}\right) = 1$ but $\langle J_1 + J_2, J_3 + J_4\rangle \neq \left\langle \begin{pmatrix}1 & 1 & 0 & 0\end{pmatrix}, \begin{pmatrix}0 & 0 & 1 & 1\end{pmatrix}\right\rangle$. After trying all cases, we concluded that this situation never happens.

5.2. A simple result on the θ-congruent number problem for $\theta = \cos^{-1}\left(\frac{1}{4}\right)$

In this Section, we show an example of how to apply generalized Monsky matrices on problems other that the congruent number problem in order to find new results.

We chose to work with $\theta = \cos^{-1}\left(\frac{1}{4}\right)$ because it is one of the angles with the simplest cosine other that $\frac{\pi}{2}$, $\frac{\pi}{3}$ and $\frac{2\pi}{3}$.

We prove a result similar to Iskra's theorem on congruent numbers presented in Theorem 0.2.6:

Theorem 5.2.1. *Let* $\theta = \cos^{-1}\left(\frac{1}{4}\right)$ *and* ℓ *be a positive integer. If* $p_1, p_2, \ldots p_{2\ell}$ *are distinct primes congruent to 17 modulo 120 such that* $\left(\frac{p_i}{p_j}\right) = 1$ *for* $i < j$*, then* $n = 2p_1p_2 \cdots p_{2\ell}$ *is a non-*$\theta = \cos^{-1}\left(\frac{1}{4}\right)$*-congruent number.*

We know that, when $n \nmid 6$, n is $\cos^{-1}\left(\frac{1}{4}\right)$-congruent if and only if the elliptic curve

$$y^2 = x(x - 3n)(x + 5n)$$

has a positive rank.

With the conditions of Section 3.1, $e_2 = -8n$ and $e_3 = -3n$. Showing that $K(-8n, -3n) = 2$ will prove that n is non-$\cos^{-1}\left(\frac{1}{4}\right)$-congruent.

We can generate a family of non-$\cos^{-1}\left(\frac{1}{4}\right)$-congruent numbers by induction using Theorem 5.1.8. All we require is a base of induction:

Lemma 5.2.2. *When $n = 2$, $K(-8n, -3n) = 2$.*

Proof. When $e_2 = -16$, $e_3 = -6$ and $e_3 - e_2 = 10$, the generalized Monsky matrix is

$$M_{-16,-6} = \left(\begin{array}{ccc|ccc} 0 & 0 & 0 & 1 & 0 & 0 \\ \hline 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 \\ \hline 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 \end{array}\right).$$

Since this is the first generalised Monsky matrix presented in this thesis, we explain its construction in detail.

The odd primes dividing $e_2e_3(e_3 - e_2)$ are 3 and 5. 3 only divides e_3 and 5 only divides $e_3 - e_2$. Using the notation from Section 4.1, we have that $q_{1_1} = -1$, $q_{1_2} = 2$, $q_{1_3} = 3$, $q_{2_1} = -1$, $q_{2_2} = 2$ and $q_{2_3} = 5$. There is no prime in the form q_{3_j} because no odd prime only divides e_2.

In the matrix, Columns 1 and 4 then represent the signs of b_1 and b_2 respectively. Columns 2 and 5 represent the parities of b_1 and b_2 respectively. Column 3 represents the 3-valuation of b_1 and Column 6 represents the 5-valuation of b_2.

Row 1 represents the condition in $\mathbb{R}$ and is given by $M_{\mathbb{R}}$ of Lemma 4.2.4.

Row 2 represents the first condition in $\mathbb{Q}_2$ and is given by the first row of $M_{\mathbb{Q}_2}$ of Lemma 4.3.15. The left side is explained by the fact that $q_{1_1} \equiv_8 7 \notin \{1,3\}$, $\overline{e_2e_3} \equiv_8 3 \notin \{5,7\}$ and $q_{1_3} \equiv_8 3 \in \{1,3\}$. The right side is explained by the fact that $\overline{e_2} \equiv_8 7 \in \{5,7\}$.

Row 3 represents the second condition in $\mathbb{Q}_2$ and is given by the second row of $M_{\mathbb{Q}_2}$ of Lemma 4.3.15. The left side is explained by the fact that $\overline{-e_2} \equiv_8 1 \notin \{5,7\}$. The right side is explained by the fact that $q_{2_1} \equiv_8 7 \notin \{1,3\}$, $\overline{-e_2e_3} \equiv_8 5 \in \{5,7\}$ and $q_{2_3} \equiv_8 5 \notin \{1,3\}$.

Row 4 represents the third condition in $\mathbb{Q}_2$ and is given by the third row of $M_{\mathbb{Q}_2}$ of Lemma 4.3.15. The left side is explained by the fact that $q_{1_1} \equiv_8 7 \notin \{1,5\}$ and

$q_{1_3} \equiv_8 3 \notin \{1,5\}$. The right side is explained by the fact that $q_{2_1} \equiv_8 7 \notin \{1,5\}$ and $q_{2_3} \equiv_8 5 \in \{1,5\}$.

Row 5 represents the condition in $\mathbb{Q}_3$ and is given by N_p of Lemma 4.4.5. The left side is explained by the fact that $q_{1_3} = 3$. The right side is explained by the fact that $\left(\frac{q_{2_1}}{3}\right) = -1$, $\left(\frac{q_{2_2}}{3}\right) = -1$ and $\left(\frac{q_{2_3}}{3}\right) = -1$.

Row 6 represents the condition in $\mathbb{Q}_5$ and is given by N_p of Lemma 4.4.6. The left side is explained by the fact that $\left(\frac{q_{1_1}}{5}\right) = 1$, $\left(\frac{q_{1_2}}{5}\right) = -1$ and $\left(\frac{q_{1_3}}{5}\right) = -1$. The left side is explained by the fact that $q_{2_3} = 5$.

One can reduce the matrix to see that its kernel is of dimension 2. This implies that $K(-16, -6) = 2$.

□

Once the basis is found, we can apply Theorem 5.1.8.

Proof of Theorem 5.2.1. This proof is done by showing that

$$K\left(-16\prod_{i=1}^{\ell} p_{2i-1}p_{2i}, -6\prod_{i=1}^{\ell} p_{2i-1}p_{2i}\right) = 2$$

for any non-negative integer ℓ. This is done by induction.

When $\ell = 0$, this is proven by Lemma 5.2.2. We proceed with the rest of the induction. Assume that the statement is true for $\ell - 1$, namely,

$$K\left(-16\prod_{i=1}^{\ell-1} p_{2i-1}p_{2i}, -6\prod_{i=1}^{\ell-1} p_{2i-1}p_{2i}\right) = 2.$$

Since $p_{2\ell-1}$ and $p_{2\ell}$ are congruent to 17 modulo 120, we have the following properties:

$$\begin{cases} \left(\dfrac{-1}{p_{2\ell-1}}\right) = \left(\dfrac{-1}{p_{2\ell}}\right) = 1, \\ \left(\dfrac{2}{p_{2\ell-1}}\right) = \left(\dfrac{2}{p_{2\ell}}\right) = 1, \\ \left(\dfrac{3}{p_{2\ell-1}}\right) = \left(\dfrac{3}{p_{2\ell}}\right) = -1, \\ \left(\dfrac{5}{p_{2\ell-1}}\right) = \left(\dfrac{5}{p_{2\ell}}\right) = -1 \end{cases}$$

We also have that, for $1 \leq i \leq 2\ell - 2$, $\left(\frac{p_i}{p_{2\ell-1}}\right) = \left(\frac{p_i}{p_{2\ell}}\right) = 1$. This implies that:

$$\begin{cases} \left(\dfrac{\overline{e_3}}{p_{2\ell-1}}\right) = \left(\dfrac{\overline{-3n}}{p_{2\ell-1}}\right) = -1, \\ \left(\dfrac{\overline{e_3 - e_2}}{p_{2\ell-1}}\right) = \left(\dfrac{\overline{5n}}{p_{2\ell-1}}\right) = -1. \end{cases}$$

We then have all the properties necessary to apply Theorem 5.1.8 and get that:

$$K\left(-16\prod_{i=1}^{\ell} p_{2i-1}p_{2i}, -6\prod_{i=1}^{\ell} p_{2i-1}p_{2i}\right) = K\left(-16\prod_{i=1}^{\ell-1} p_{2i-1}p_{2i}, -6\prod_{i=1}^{\ell-1} p_{2i-1}p_{2i}\right) = 2$$

which completes the proof by induction. □

5.3. A result on the congruent number problem

We know that, for an integer n, $K(-2n,-n) = 2$ implies that n is not a congruent number. For simplicity of notation, let us write $K'(n) := K(-2n, -n)$.

We are going to show Theorem 1.0.5, namely:

Theorem 5.3.1 (Originally Theorem 1.0.5)**.** *Let n be a square-free integer. There exists a square-free integer m such that $GCD(n,m) = 1$ and nm is non-congruent.*

Remark that we are not interested in non-square-free integers since we can always reduce to problem to the study of square-free integers.

Theorem 1.0.5 is a consequence of Theorem 5.1.9. Indeed, if our given number can be written as $n = n'p$ with p a prime congruent to 1, 3 or 5 modulo 8, then we can find a prime q such that we are able to apply Theorem 5.1.9 to show that

$K'(n') = K'(n'pq)$. Using this, we are able to reduce the problem to the study of a family of numbers whose associated generalized Monsky matrices are simple enough to be worked on explicitly.

There are two complications that will make the proof a bit longer that we would wish. Firstly, this idea cannot be applied to primes congruent to 7 modulo 8 because, for such primes p, we have that $\left(\frac{2}{p}\right) = 1$ and, since $e_2 = -2n$ and $e_3 = -n$, this guarantees that $\left(\frac{e_3}{p}\right) = \left(\frac{e_2}{p}\right)$ which prevents us from applying Theorem 5.1.9. The other complication is that, when $p \equiv_8 1$ or 5, we need that $\left(\frac{n}{p}\right) = -1$, which is not always the case. This complication can be resolved by multiplying n by a prime congruent to 7 modulo 8 that will cause the desired Legendre symbols to be negative.

Because of the complications described above, there are several cases in the proof of this theorem. We have found that it is more efficient to give an algorithm finding the right multiple instead of doing the proof case by case. At the end of the algorithm, the constructed multiple will always have the same general form.

Proof of Theorem 5.3.1. If n is already non-congruent, multiply n by any relatively prime number. If this new number is still non-congruent, we are done. If not, we work with that new number using the following proof.

We start by factorizing n as:

$$n = 2^{\varepsilon_1} 3^{\varepsilon_2} \prod_{i \in \{1,3,5,7\}} \prod_{j=1}^{\ell_i} p_{i,j}$$

with ε_1,$\varepsilon_2 \in \{0,1\}$ and $p_{i,j} \equiv_8 i$.

The following algorithm generates m:

Algorithm 1 Generation of m

```
procedure GENERATION OF $m(n)$
    $m \leftarrow 1$
    if $2 \nmid n$ then
        $m \leftarrow 2 \times m$
    if $3 \nmid n$ then
        $m \leftarrow 3 \times m$
    $n' \leftarrow n \times m$
    for $j$ from 1 to $\ell_3$ do
        Find a prime $q$ not dividing $nm$ congruent to $3 \mod 8$ such that $\left(\frac{p}{q}\right) = \left(\frac{p}{p_{3,j}}\right)$ for all primes $p$ dividing $nm$ (other than $p_{3,j}$).
        $m \leftarrow q \times m$
        $q_{3,j} \leftarrow q$
    for $i \in \{1,5\}$ do
        for $j$ from 1 to $\ell_i$ do
            Find a prime $q$ not dividing $nm$ congruent to $i \mod 8$ such that, for all odd primes $p$ dividing $nm$ other than $p_{i,j}$, $\left(\frac{p}{q}\right) = \left(\frac{p}{p_{i,j}}\right)$.
            $m \leftarrow q \times m$
            $q_{i,j} \leftarrow q$
    Find a prime $q$ not dividing $nm$ congruent to $7 \mod 8$ such that, for all odd primes $p_{i,j}$ and $q_{i,j}$ dividing $nm$ with $i \in \{1,3,5\}$, $\left(\frac{q_{i,j}}{q}\right) = \left(\frac{p_{i,j}}{q}\right)$ and $\left(\frac{q}{p_{i,j}}\right) = -\left(\frac{n}{p_{i,j}}\right)$.
    $m \leftarrow q \times m$
    $p_{7,\ell_7+1} \leftarrow q$
    $\ell_7 \leftarrow \ell_7 + 1$
    if $2 \mid \ell_7$ then
        Find a prime $q$ not dividing $nm$ congruent to $7 \mod 8$ such that, for all odd primes $p$ dividing $nm$ not congruent to $7 \mod 8$, $\left(\frac{q}{p}\right) = 1$.
        $m \leftarrow q \times m$
        $p_{7,\ell_7+1} \leftarrow q$
        $\ell_7 \leftarrow \ell_7 + 1$
    for $j$ from 1 to $\ell_7$ do
        Find a prime $q$ not dividing $nm$ congruent to $17 \mod 24$ such that, for all primes $p$ dividing $nm$ but not $6p_{7,j}$, $\left(\frac{q}{p}\right) = 1$ and $\left(\frac{q}{p_{7,j}}\right) = -1$.
        $m \leftarrow q \times m$
        $q'_{1,j} \leftarrow q$
    return $m$
```

We first remark that the algorithm always returns a number. We now justify the part where we ask to find new primes with certain congruence conditions. Because of Dirichlet's theorem on arithmetic progressions and the Chinese Reminder Theorem, we are guaranteed that such primes always exist. It remains to show that nm is non-congruent.

We have that nm can be factorized as:

$$nm = 6\left(\prod_{j=1}^{\ell_1} p_{1,j}q_{1,j}\right)\left(\prod_{j=1}^{\ell_3} p_{3,j}q_{3,j}\right)\left(\prod_{j=1}^{\ell_5} p_{5,j}q_{5,j}\right)\left(\prod_{j=1}^{\ell_7} p_{7,j}q'_{1,j}\right).$$

We will now apply Theorem 5.1.9 multiple times. We first remark that the theorem implies that:

$$\begin{aligned} &K'\left(6\left(\prod_{j=1}^{\ell_1} p_{1,j}q_{1,j}\right)\left(\prod_{j=1}^{\ell_3} p_{3,j}q_{3,j}\right)\left(\prod_{j=1}^{\ell_5} p_{5,j}q_{5,j}\right)\left(\prod_{j=1}^{\ell_7} p_{7,j}q'_{1,j}\right)\right) \\ &\quad = K'\left(6\left(\prod_{j=1}^{\ell_1-1} p_{1,j}q_{1,j}\right)\left(\prod_{j=1}^{\ell_3} p_{3,j}q_{3,j}\right)\left(\prod_{j=1}^{\ell_5} p_{5,j}q_{5,j}\right)\left(\prod_{j=1}^{\ell_7} p_{7,j}q'_{1,j}\right)\right). \end{aligned}$$

Since we remove two primes each time and these primes have the same Legendre symbols with other primes, the Legendre symbol of the product over each prime does not change. Using this, we can remove the entire first subproduct by simply reapplying Corollary 5.1.9 enough times and get

$$K'(nm) = K'\left(6\left(\prod_{j=1}^{\ell_3} p_{3,j}q_{3,j}\right)\left(\prod_{j=1}^{\ell_5} p_{5,j}q_{5,j}\right)\left(\prod_{j=1}^{\ell_7} p_{7,j}q'_{1,j}\right)\right).$$

We can do the same thing to the primes congruent to $5 \mod 8$ and then to those congruent to $3 \mod 8$ to get that

$$K'(nm) = K'\left(6\left(\prod_{j=1}^{\ell_7} p_{7,j}q'_{1,j}\right)\right).$$

The algorithm guarantees that ℓ_7 is odd. All that is left to do is to show that $K'\left(6\left(\prod_{j=1}^{\ell_7} p_{7,j}q'_{1,j}\right)\right) = 2$. This will be done in Lemma 5.3.2 that follows this proof. Lemma 5.3.2 implies that the integer nm created by Algorithm 1 has

$$K'\left(nm\right) = K'\left(6\left(\prod_{j=1}^{\ell_7} p_{7,j}q'_{1,j}\right)\right) = 2.$$

This concludes the proof of Theorem 5.3.1.

□

Lemma 5.3.2 (Originally Lemma 1.0.2)**.** *Let n be a square-free integer that can be factorized as*

$$n = 6p_1 \cdots p_t q_1 \cdots q_t,$$

with

$$\begin{cases} 2 \nmid t, \\ \forall i, p_i \equiv_8 7, \\ \forall i, q_i \equiv_8 1, \\ \forall i, \left(\dfrac{p_i}{q_i}\right) = -1, \\ \forall i \neq j, \left(\dfrac{p_i}{q_j}\right) = \left(\dfrac{q_i}{q_j}\right) = 1, \\ \forall i, \left(\dfrac{3}{q_i}\right) = -1. \end{cases}$$

Then we have that $K(-2n, -n) = 2$.

Proof. Observe that:

$$M_{-2n,-n} =$$

$$\left(\begin{array}{cc|c|ccccc|ccccc||cc|c|ccccc|ccccc}
0 & 0 & 0 & 0 & 0 & 0 & \dots & 0 & 0 & 0 & 0 & \dots & 0 & 1 & 0 & 0 & 0 & 0 & 0 & \dots & 0 & 0 & 0 & 0 & \dots & 0 \\
\hline
1 & 0 & 0 & 1 & 1 & 1 & \dots & 1 & 0 & 0 & 0 & \dots & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \dots & 0 & 0 & 0 & 0 & \dots & 0 \\
\hline
0 & 1 & 0 & 0 & 0 & 0 & \dots & 0 & 0 & 0 & 0 & \dots & 0 & 0 & 0 & 1 & 0 & 0 & 0 & \dots & 0 & 0 & 0 & 0 & \dots & 0 \\
\hline
1 & 0 & 1 & 1 & 1 & 1 & \dots & 1 & 0 & 0 & 0 & \dots & 0 & 1 & 1 & 1 & 1 & 1 & 1 & \dots & 1 & 0 & 0 & 0 & \dots & 0 \\
\hline\hline
1 & 1 & \ast & \ast & \ast & \ast & \dots & \ast & 1 & 1 & 1 & \dots & 1 & 0 & 0 & 1 & 0 & 0 & 0 & \dots & 0 & 0 & 0 & 0 & \dots & 0 \\
\hline
1 & 0 & \ast & \ast & \ast & \ast & \dots & \ast & 1 & 0 & 0 & \dots & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \dots & 0 & 0 & 0 & 0 & \dots & 0 \\
1 & 0 & \ast & \ast & \ast & \ast & \dots & \ast & 0 & 1 & 0 & \dots & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \dots & 0 & 0 & 0 & 0 & \dots & 0 \\
1 & 0 & \ast & \ast & \ast & \ast & \dots & \ast & 0 & 0 & 1 & \dots & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \dots & 0 & 0 & 0 & 0 & \dots & 0 \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\
1 & 0 & \ast & \ast & \ast & \ast & \dots & \ast & 0 & 0 & 0 & \dots & 1 & 0 & 0 & 0 & 0 & 0 & 0 & \dots & 0 & 0 & 0 & 0 & \dots & 0 \\
\hline
0 & 0 & 1 & 1 & 0 & 0 & \dots & 0 & 0 & 0 & 0 & \dots & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \dots & 0 & 0 & 0 & 0 & \dots & 0 \\
0 & 0 & 1 & 0 & 1 & 0 & \dots & 0 & 0 & 0 & 0 & \dots & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \dots & 0 & 0 & 0 & 0 & \dots & 0 \\
0 & 0 & 1 & 0 & 0 & 1 & \dots & 0 & 0 & 0 & 0 & \dots & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \dots & 0 & 0 & 0 & 0 & \dots & 0 \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\
0 & 0 & 1 & 0 & 0 & 0 & \dots & 1 & 0 & 0 & 0 & \dots & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \dots & 0 & 0 & 0 & 0 & \dots & 0 \\
\hline\hline
0 & 0 & 1 & 0 & 0 & 0 & \dots & 0 & 0 & 0 & 0 & \dots & 0 & 1 & 1 & \ast & \ast & \ast & \ast & \dots & \ast & 1 & 1 & 1 & \dots & 1 \\
\hline
0 & 0 & 0 & 0 & 0 & 0 & \dots & 0 & 0 & 0 & 0 & \dots & 0 & 1 & 0 & \ast & \ast & \ast & \ast & \dots & \ast & 1 & 0 & 0 & \dots & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & \dots & 0 & 0 & 0 & 0 & \dots & 0 & 1 & 0 & \ast & \ast & \ast & \ast & \dots & \ast & 0 & 1 & 0 & \dots & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & \dots & 0 & 0 & 0 & 0 & \dots & 0 & 1 & 0 & \ast & \ast & \ast & \ast & \dots & \ast & 0 & 0 & 1 & \dots & 0 \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\
0 & 0 & 0 & 0 & 0 & 0 & \dots & 0 & 0 & 0 & 0 & \dots & 0 & 1 & 0 & \ast & \ast & \ast & \ast & \dots & \ast & 0 & 0 & 0 & \dots & 1 \\
\hline
0 & 0 & 0 & 0 & 0 & 0 & \dots & 0 & 0 & 0 & 0 & \dots & 0 & 0 & 0 & 1 & 1 & 0 & 0 & \dots & 0 & 0 & 0 & 0 & \dots & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & \dots & 0 & 0 & 0 & 0 & \dots & 0 & 0 & 0 & 1 & 0 & 1 & 0 & \dots & 0 & 0 & 0 & 0 & \dots & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & \dots & 0 & 0 & 0 & 0 & \dots & 0 & 0 & 0 & 1 & 0 & 0 & 1 & \dots & 0 & 0 & 0 & 0 & \dots & 0 \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\
0 & 0 & 0 & 0 & 0 & 0 & \dots & 0 & 0 & 0 & 0 & \dots & 0 & 0 & 0 & 1 & 0 & 0 & 0 & \dots & 1 & 0 & 0 & 0 & \dots & 0
\end{array}\right)$$

We number the matrix rows and columns using the above matrix representation.

Columns 1 and 14 represent the signs of b_1 and b_2 respectively. Columns 2 and 15 represent the parities of b_1 and b_2 respectively. Columns 3 and 16 represent the 3-valuations of b_1 and b_2 respectively. Columns 4 to 8 represent the p_i-valuations of

b_1. Columns 9 to 13 represent the q_i-valuations of b_1. Columns 17 to 21 represent the p_i-valuations of b_2. Columns 22 to 26 represent the q_i-valuations of b_2.

The first row represents the condition for a solution in $\mathbb{R}$ and is obtained by using $M_{\mathbb{R}}$ of Lemma 4.2.4. Rows 2 to 4 represent the conditions for a solution in $\mathbb{Q}_2$ and are obtained by using $M_{\mathbb{Q}_2}$ of Lemma 4.3.12. Row 5 represents the condition on b_1 for a solution in $\mathbb{Q}_3$ are is obtained by using $N_{p,1}$ of Lemma 4.4.8. Rows 6 to 10 represent the conditions on b_1 for a solution in $\mathbb{Q}_{p_i}$ and are obtained by using $N_{p,1}$ of Lemma 4.4.8. Rows 11 to 15 represent the conditions on b_1 for a solution in $\mathbb{Q}_{q_i}$ and are obtained by using $N_{p,1}$ of Lemma 4.4.8. Row 16 represents the condition on b_2 for a solution in $\mathbb{Q}_3$ are is obtained by using $N_{p,2}$ of Lemma 4.4.8. Rows 17 to 21 represent the conditions on b_2 for a solution in $\mathbb{Q}_{p_i}$ and are obtained by using $N_{p,2}$ of Lemma 4.4.8. Rows 22 to 26 represent the conditions on b_2 for a solution in $\mathbb{Q}_{q_i}$ and are obtained by using $N_{p,2}$ of Lemma 4.4.8.

In the following pages we will show that if we remove Rows 3 and 4 from the matrix, the rest of the rows are linearly independent. Indeed, when we remove Rows 3 and 4 from the matrix, we get the following submatrix:

$$\left(\begin{array}{cc|c|ccccc|ccccc||cc|c|ccccc|ccccc}
0 & 0 & 0 & 0 & 0 & 0 & \ldots & 0 & 0 & 0 & 0 & \ldots & 0 & 1 & 0 & 0 & 0 & 0 & 0 & \ldots & 0 & 0 & 0 & 0 & \ldots & 0 \\
\hline
1 & 0 & 0 & 1 & 1 & 1 & \ldots & 1 & 0 & 0 & 0 & \ldots & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \ldots & 0 & 0 & 0 & 0 & \ldots & 0 \\
\hline\hline
1 & 1 & \ast & \ast & \ast & \ast & \ldots & \ast & 1 & 1 & 1 & \ldots & 1 & 0 & 0 & 1 & 0 & 0 & 0 & \ldots & 0 & 0 & 0 & 0 & \ldots & 0 \\
\hline
1 & 0 & \ast & \ast & \ast & \ast & \ldots & \ast & 1 & 0 & 0 & \ldots & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \ldots & 0 & 0 & 0 & 0 & \ldots & 0 \\
1 & 0 & \ast & \ast & \ast & \ast & \ldots & \ast & 0 & 1 & 0 & \ldots & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \ldots & 0 & 0 & 0 & 0 & \ldots & 0 \\
1 & 0 & \ast & \ast & \ast & \ast & \ldots & \ast & 0 & 0 & 1 & \ldots & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \ldots & 0 & 0 & 0 & 0 & \ldots & 0 \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\
1 & 0 & \ast & \ast & \ast & \ast & \ldots & \ast & 0 & 0 & 0 & \ldots & 1 & 0 & 0 & 0 & 0 & 0 & 0 & \ldots & 0 & 0 & 0 & 0 & \ldots & 0 \\
\hline
0 & 0 & 1 & 1 & 0 & 0 & \ldots & 0 & 0 & 0 & 0 & \ldots & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \ldots & 0 & 0 & 0 & 0 & \ldots & 0 \\
0 & 0 & 1 & 0 & 1 & 0 & \ldots & 0 & 0 & 0 & 0 & \ldots & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \ldots & 0 & 0 & 0 & 0 & \ldots & 0 \\
0 & 0 & 1 & 0 & 0 & 1 & \ldots & 0 & 0 & 0 & 0 & \ldots & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \ldots & 0 & 0 & 0 & 0 & \ldots & 0 \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\
0 & 0 & 1 & 0 & 0 & 0 & \ldots & 1 & 0 & 0 & 0 & \ldots & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \ldots & 0 & 0 & 0 & 0 & \ldots & 0 \\
\hline\hline
0 & 0 & 1 & 0 & 0 & 0 & \ldots & 0 & 0 & 0 & 0 & \ldots & 0 & 1 & 1 & \ast & \ast & \ast & \ast & \ldots & \ast & 1 & 1 & 1 & \ldots & 1 \\
\hline
0 & 0 & 0 & 0 & 0 & 0 & \ldots & 0 & 0 & 0 & 0 & \ldots & 0 & 1 & 0 & \ast & \ast & \ast & \ast & \ldots & \ast & 1 & 0 & 0 & \ldots & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & \ldots & 0 & 0 & 0 & 0 & \ldots & 0 & 1 & 0 & \ast & \ast & \ast & \ast & \ldots & \ast & 0 & 1 & 0 & \ldots & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & \ldots & 0 & 0 & 0 & 0 & \ldots & 0 & 1 & 0 & \ast & \ast & \ast & \ast & \ldots & \ast & 0 & 0 & 1 & \ldots & 0 \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\
0 & 0 & 0 & 0 & 0 & 0 & \ldots & 0 & 0 & 0 & 0 & \ldots & 0 & 1 & 0 & \ast & \ast & \ast & \ast & \ldots & \ast & 0 & 0 & 0 & \ldots & 1 \\
\hline
0 & 0 & 0 & 0 & 0 & 0 & \ldots & 0 & 0 & 0 & 0 & \ldots & 0 & 0 & 0 & 1 & 1 & 0 & 0 & \ldots & 0 & 0 & 0 & 0 & \ldots & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & \ldots & 0 & 0 & 0 & 0 & \ldots & 0 & 0 & 0 & 1 & 0 & 1 & 0 & \ldots & 0 & 0 & 0 & 0 & \ldots & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & \ldots & 0 & 0 & 0 & 0 & \ldots & 0 & 0 & 0 & 1 & 0 & 0 & 1 & \ldots & 0 & 0 & 0 & 0 & \ldots & 0 \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\
0 & 0 & 0 & 0 & 0 & 0 & \ldots & 0 & 0 & 0 & 0 & \ldots & 0 & 0 & 0 & 1 & 0 & 0 & 0 & \ldots & 1 & 0 & 0 & 0 & \ldots & 0
\end{array}\right)$$

Using the above matrix representation, we remark that Row 3 is LI since it is the only row with a 1 on the second column in the above matrix representation. Similarly, Row 14 is LI because it is the only row with a 1 on Column 15. We can then remove both and check the remaining rows:

$$\left(\begin{array}{cc|c|ccccc|ccccc||cc|c|ccccc|ccccc}
0 & 0 & 0 & 0 & 0 & 0 & \dots & 0 & 0 & 0 & 0 & \dots & 0 & 1 & 0 & 0 & 0 & 0 & 0 & \dots & 0 & 0 & 0 & 0 & \dots & 0 \\
\hline
1 & 0 & 0 & 1 & 1 & 1 & \dots & 1 & 0 & 0 & 0 & \dots & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \dots & 0 & 0 & 0 & 0 & \dots & 0 \\
\hline\hline
1 & 0 & \ast & \ast & \ast & \ast & \dots & \ast & 1 & 0 & 0 & \dots & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \dots & 0 & 0 & 0 & 0 & \dots & 0 \\
1 & 0 & \ast & \ast & \ast & \ast & \dots & \ast & 0 & 1 & 0 & \dots & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \dots & 0 & 0 & 0 & 0 & \dots & 0 \\
1 & 0 & \ast & \ast & \ast & \ast & \dots & \ast & 0 & 0 & 1 & \dots & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \dots & 0 & 0 & 0 & 0 & \dots & 0 \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\
1 & 0 & \ast & \ast & \ast & \ast & \dots & \ast & 0 & 0 & 0 & \dots & 1 & 0 & 0 & 0 & 0 & 0 & 0 & \dots & 0 & 0 & 0 & 0 & \dots & 0 \\
\hline
0 & 0 & 1 & 1 & 0 & 0 & \dots & 0 & 0 & 0 & 0 & \dots & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \dots & 0 & 0 & 0 & 0 & \dots & 0 \\
0 & 0 & 1 & 0 & 1 & 0 & \dots & 0 & 0 & 0 & 0 & \dots & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \dots & 0 & 0 & 0 & 0 & \dots & 0 \\
0 & 0 & 1 & 0 & 0 & 1 & \dots & 0 & 0 & 0 & 0 & \dots & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \dots & 0 & 0 & 0 & 0 & \dots & 0 \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\
0 & 0 & 1 & 0 & 0 & 0 & \dots & 1 & 0 & 0 & 0 & \dots & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \dots & 0 & 0 & 0 & 0 & \dots & 0 \\
\hline\hline
0 & 0 & 0 & 0 & 0 & 0 & \dots & 0 & 0 & 0 & 0 & \dots & 0 & 1 & 0 & \ast & \ast & \ast & \ast & \dots & \ast & 1 & 0 & 0 & \dots & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & \dots & 0 & 0 & 0 & 0 & \dots & 0 & 1 & 0 & \ast & \ast & \ast & \ast & \dots & \ast & 0 & 1 & 0 & \dots & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & \dots & 0 & 0 & 0 & 0 & \dots & 0 & 1 & 0 & \ast & \ast & \ast & \ast & \dots & \ast & 0 & 0 & 1 & \dots & 0 \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\
0 & 0 & 0 & 0 & 0 & 0 & \dots & 0 & 0 & 0 & 0 & \dots & 0 & 1 & 0 & \ast & \ast & \ast & \ast & \dots & \ast & 0 & 0 & 0 & \dots & 1 \\
\hline
0 & 0 & 0 & 0 & 0 & 0 & \dots & 0 & 0 & 0 & 0 & \dots & 0 & 0 & 0 & 1 & 1 & 0 & 0 & \dots & 0 & 0 & 0 & 0 & \dots & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & \dots & 0 & 0 & 0 & 0 & \dots & 0 & 0 & 0 & 1 & 0 & 1 & 0 & \dots & 0 & 0 & 0 & 0 & \dots & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & \dots & 0 & 0 & 0 & 0 & \dots & 0 & 0 & 0 & 1 & 0 & 0 & 1 & \dots & 0 & 0 & 0 & 0 & \dots & 0 \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\
0 & 0 & 0 & 0 & 0 & 0 & \dots & 0 & 0 & 0 & 0 & \dots & 0 & 0 & 0 & 1 & 0 & 0 & 0 & \dots & 1 & 0 & 0 & 0 & \dots & 0
\end{array}\right)$$

Using the above matrix representation, we remark that the Rows 3 to 7 are LI from the rest and themselves because they are the only rows with a 1 in Columns 9 to 13 respectively. We can then remove them and check the remaining rows:

$$\left(\begin{array}{cc|c|ccccc|ccccc||cc|c|ccccc|ccccc}
0 & 0 & 0 & 0 & 0 & 0 & \dots & 0 & 0 & 0 & 0 & \dots & 0 & 1 & 0 & 0 & 0 & 0 & 0 & \dots & 0 & 0 & 0 & 0 & \dots & 0 \\
\hline
1 & 0 & 0 & 1 & 1 & 1 & \dots & 1 & 0 & 0 & 0 & \dots & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \dots & 0 & 0 & 0 & 0 & \dots & 0 \\
\hline\hline
0 & 0 & 1 & 1 & 0 & 0 & \dots & 0 & 0 & 0 & 0 & \dots & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \dots & 0 & 0 & 0 & 0 & \dots & 0 \\
0 & 0 & 1 & 0 & 1 & 0 & \dots & 0 & 0 & 0 & 0 & \dots & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \dots & 0 & 0 & 0 & 0 & \dots & 0 \\
0 & 0 & 1 & 0 & 0 & 1 & \dots & 0 & 0 & 0 & 0 & \dots & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \dots & 0 & 0 & 0 & 0 & \dots & 0 \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\
0 & 0 & 1 & 0 & 0 & 0 & \dots & 1 & 0 & 0 & 0 & \dots & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \dots & 0 & 0 & 0 & 0 & \dots & 0 \\
\hline\hline
0 & 0 & 0 & 0 & 0 & 0 & \dots & 0 & 0 & 0 & 0 & \dots & 0 & 1 & 0 & \ast & \ast & \ast & \ast & \dots & \ast & 1 & 0 & 0 & \dots & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & \dots & 0 & 0 & 0 & 0 & \dots & 0 & 1 & 0 & \ast & \ast & \ast & \ast & \dots & \ast & 0 & 1 & 0 & \dots & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & \dots & 0 & 0 & 0 & 0 & \dots & 0 & 1 & 0 & \ast & \ast & \ast & \ast & \dots & \ast & 0 & 0 & 1 & \dots & 0 \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\
0 & 0 & 0 & 0 & 0 & 0 & \dots & 0 & 0 & 0 & 0 & \dots & 0 & 1 & 0 & \ast & \ast & \ast & \ast & \dots & \ast & 0 & 0 & 0 & \dots & 1 \\
\hline
0 & 0 & 0 & 0 & 0 & 0 & \dots & 0 & 0 & 0 & 0 & \dots & 0 & 0 & 0 & 1 & 1 & 0 & 0 & \dots & 0 & 0 & 0 & 0 & \dots & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & \dots & 0 & 0 & 0 & 0 & \dots & 0 & 0 & 0 & 1 & 0 & 1 & 0 & \dots & 0 & 0 & 0 & 0 & \dots & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & \dots & 0 & 0 & 0 & 0 & \dots & 0 & 0 & 0 & 1 & 0 & 0 & 1 & \dots & 0 & 0 & 0 & 0 & \dots & 0 \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\
0 & 0 & 0 & 0 & 0 & 0 & \dots & 0 & 0 & 0 & 0 & \dots & 0 & 0 & 0 & 1 & 0 & 0 & 0 & \dots & 1 & 0 & 0 & 0 & \dots & 0
\end{array}\right)$$

Using the above matrix representation, we remark that the Rows 8 to 12 are LI from the rest and themselves because they are the only rows with a 1 in Columns 22 to 26 respectively. We can then remove them and check the remaining rows:

$$\left(\begin{array}{cc|c|ccccc|ccccc||cc|c|ccccc|ccccc}
0 & 0 & 0 & 0 & 0 & 0 & \dots & 0 & 0 & 0 & 0 & \dots & 0 & 1 & 0 & 0 & 0 & 0 & 0 & \dots & 0 & 0 & 0 & 0 & \dots & 0 \\
\hline
1 & 0 & 0 & 1 & 1 & 1 & \dots & 1 & 0 & 0 & 0 & \dots & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \dots & 0 & 0 & 0 & 0 & \dots & 0 \\
\hline\hline
0 & 0 & 1 & 1 & 0 & 0 & \dots & 0 & 0 & 0 & 0 & \dots & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \dots & 0 & 0 & 0 & 0 & \dots & 0 \\
0 & 0 & 1 & 0 & 1 & 0 & \dots & 0 & 0 & 0 & 0 & \dots & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \dots & 0 & 0 & 0 & 0 & \dots & 0 \\
0 & 0 & 1 & 0 & 0 & 1 & \dots & 0 & 0 & 0 & 0 & \dots & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \dots & 0 & 0 & 0 & 0 & \dots & 0 \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\
0 & 0 & 1 & 0 & 0 & 0 & \dots & 1 & 0 & 0 & 0 & \dots & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \dots & 0 & 0 & 0 & 0 & \dots & 0 \\
\hline\hline
0 & 0 & 0 & 0 & 0 & 0 & \dots & 0 & 0 & 0 & 0 & \dots & 0 & 0 & 0 & 1 & 1 & 0 & 0 & \dots & 0 & 0 & 0 & 0 & \dots & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & \dots & 0 & 0 & 0 & 0 & \dots & 0 & 0 & 0 & 1 & 0 & 1 & 0 & \dots & 0 & 0 & 0 & 0 & \dots & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & \dots & 0 & 0 & 0 & 0 & \dots & 0 & 0 & 0 & 1 & 0 & 0 & 1 & \dots & 0 & 0 & 0 & 0 & \dots & 0 \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\
0 & 0 & 0 & 0 & 0 & 0 & \dots & 0 & 0 & 0 & 0 & \dots & 0 & 0 & 0 & 1 & 0 & 0 & 0 & \dots & 1 & 0 & 0 & 0 & \dots & 0
\end{array}\right)$$

We then remark that the second row is LI since it is the only row with a 1 on the first column in the above matrix representation. We then remove it and check the other rows:

$$\left(\begin{array}{cc|c|ccccc|ccccc||cc|c|ccccc|ccccc}
0 & 0 & 0 & 0 & 0 & 0 & \dots & 0 & 0 & 0 & 0 & \dots & 0 & 1 & 0 & 0 & 0 & 0 & 0 & \dots & 0 & 0 & 0 & 0 & \dots & 0 \\
\hline\hline
0 & 0 & 1 & 1 & 0 & 0 & \dots & 0 & 0 & 0 & 0 & \dots & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \dots & 0 & 0 & 0 & 0 & \dots & 0 \\
0 & 0 & 1 & 0 & 1 & 0 & \dots & 0 & 0 & 0 & 0 & \dots & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \dots & 0 & 0 & 0 & 0 & \dots & 0 \\
0 & 0 & 1 & 0 & 0 & 1 & \dots & 0 & 0 & 0 & 0 & \dots & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \dots & 0 & 0 & 0 & 0 & \dots & 0 \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\
0 & 0 & 1 & 0 & 0 & 0 & \dots & 1 & 0 & 0 & 0 & \dots & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \dots & 0 & 0 & 0 & 0 & \dots & 0 \\
\hline\hline
0 & 0 & 0 & 0 & 0 & 0 & \dots & 0 & 0 & 0 & 0 & \dots & 0 & 0 & 0 & 1 & 1 & 0 & 0 & \dots & 0 & 0 & 0 & 0 & \dots & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & \dots & 0 & 0 & 0 & 0 & \dots & 0 & 0 & 0 & 1 & 0 & 1 & 0 & \dots & 0 & 0 & 0 & 0 & \dots & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & \dots & 0 & 0 & 0 & 0 & \dots & 0 & 0 & 0 & 1 & 0 & 0 & 1 & \dots & 0 & 0 & 0 & 0 & \dots & 0 \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\
0 & 0 & 0 & 0 & 0 & 0 & \dots & 0 & 0 & 0 & 0 & \dots & 0 & 0 & 0 & 1 & 0 & 0 & 0 & \dots & 1 & 0 & 0 & 0 & \dots & 0
\end{array}\right)$$

We then remark that the first row is LI since it is the only row with a 1 on the 14th column in the above matrix representation. We then remove it and check the other rows:

$$\left(\begin{array}{cc|c|ccccc|ccccc||cc|c|ccccc|ccccc}
0&0&1&1&0&0&\dots&0&0&0&0&\dots&0&0&0&0&0&0&0&\dots&0&0&0&0&\dots&0\\
0&0&1&0&1&0&\dots&0&0&0&0&\dots&0&0&0&0&0&0&0&\dots&0&0&0&0&\dots&0\\
0&0&1&0&0&1&\dots&0&0&0&0&\dots&0&0&0&0&0&0&0&\dots&0&0&0&0&\dots&0\\
\vdots&\vdots&\vdots&\vdots&\vdots&\vdots&\ddots&\vdots&\vdots&\vdots&\vdots&\ddots&\vdots&\vdots&\vdots&\vdots&\vdots&\vdots&\vdots&\ddots&\vdots&\vdots&\vdots&\vdots&\ddots&\vdots\\
0&0&1&0&0&0&\dots&1&0&0&0&\dots&0&0&0&0&0&0&0&\dots&0&0&0&0&\dots&0\\
\hline\hline
0&0&0&0&0&0&\dots&0&0&0&0&\dots&0&0&0&1&1&0&0&\dots&0&0&0&0&\dots&0\\
0&0&0&0&0&0&\dots&0&0&0&0&\dots&0&0&0&1&0&1&0&\dots&0&0&0&0&\dots&0\\
0&0&0&0&0&0&\dots&0&0&0&0&\dots&0&0&0&1&0&0&1&\dots&0&0&0&0&\dots&0\\
\vdots&\vdots&\vdots&\vdots&\vdots&\vdots&\ddots&\vdots&\vdots&\vdots&\vdots&\ddots&\vdots&\vdots&\vdots&\vdots&\vdots&\vdots&\vdots&\ddots&\vdots&\vdots&\vdots&\vdots&\ddots&\vdots\\
0&0&0&0&0&0&\dots&0&0&0&0&\dots&0&0&0&1&0&0&0&\dots&1&0&0&0&\dots&0
\end{array}\right)$$

All the remaining rows are linearly independent. Indeed, using the above matrix representation, Rows 1 to 5 are linearly independent since they are the only ones with a 1 in Columns 4 to 8. Rows 6 to 10 are also LI because they are the only rows with a 1 in Columns 17 to 21 respectively.

With this, we have shown that every row but two of $M_{-2n,-n}$ are linearly independent. This implies that $K(-2n,-n) = 2$ and concludes the proof of Lemma 5.3.2.

□

Conclusion

As shown in this thesis, generalized Monsky matrices can be used to find new results around the congruent number problem and its generalisations.

An important consequence of Monsky matrices is Theorem 5.1.9. This result can be used to find a non-trivial infinite family of zero rank elliptic curves for any given zero rank elliptic curve. As seen in Section 5.2, Theorem 5.1.9 makes it easy to prove new statements similar to Iskra's result on congruent numbers presented in Theorem 0.2.6.

Another important result coming from generalized Monsky matrices is Theorem 5.3.1. This statement can probably be adapted on non-θ-congruent numbers for any given θ with rational cosine.

We end this thesis by presenting one of the conjectures deriving from Theorem 5.3.1 and some possible ways to prove it.

Conjecture 5.3.3. *Let n be a square-free integer. There exists a square-free integer m such that $GCD(n,m) = 1$ and nm is $\frac{\pi}{3}$-non-congruent.*

In order to prove this conjecture, one could start by developing an algorithm similar to Algorithm 1 and then apply Theorem 5.1.9 to reduce nm to a product of primes congruent to 2 or 3 modulo 4.

There are two major complications that appear here. The first complication is that 3 divides e_3. Because of this, we would need to consider primes congruent to 1 modulo 3 separately from primes congruent to 2 modulo 3. Instead of separating the primes in four sets depending on their congruence modulo 8 as in the proof of Theorem 5.3.1, we would have to separate them in eight sets depending on their congruent modulo 24. This more than doubles the work to be done as well as the size of the generalized Monsky matrix.

The other complication comes from the fact that the $\frac{\pi}{3}$-congruent number problem has $e_2 = 4n$, $e_3 = 3n$ and $e_3 - e_2 = -n$. One can verify that Theorem 5.1.9 does not apply in this case for primes congruent to 3 modulo 4.

There are two possible ways to solve these complications. The first way would be to generalise Theorem 5.1.9 for new sets of primes and find a set that applies to primes congruent to 3 modulo 4 in the $\frac{\pi}{3}$-congruent number problem. The other way would be to find a non-congruent family of non-$\frac{\pi}{3}$-congruent numbers containing prime factors congruent to 3, 7, 1 and 23 modulo 24 and use this family as the basis of induction.

Appendix A

Algorithms to verify the conditions of Section 3.3

We present here two algorithms to check that the conditions given in Theorems 3.3.1, 3.3.2, 3.3.3 and 3.3.4 are necessary and sufficient respectively for the equation system

$$\begin{cases} b_1 z_1^2 - b_2 z_2^2 = e_2 d^2, \\ b_1 z_1^2 - b_1 b_2 z_3^2 = e_3 d^2, \end{cases}$$

to have a solution in $\mathbb{Z}/2^q\mathbb{Z}$ with $2 \nmid GCD(z_1,z_2,z_3,d)$. These algorithms can be used to verify any given condition and were used to show that the conditions of Section 3.3 are both necessary and sufficient.

For the given algorithms, we will suppose that the conditions are represented as a propositional function $C(e_2,e_3,b_1,b_2)$ that returns True if (b_1,b_2) respects our conditions and False if not.

We need three simple functions. The first is the function $GCD(a_1,\ldots,a_n)$ that calculates the greatest common divisor of the integers given as parameters. The second is SQUARES(n) that gives the subset of squares in $\mathbb{Z}/n\mathbb{Z}$. The third is FOURPOWERS(n) that gives the powers of 4 in $\mathbb{Z}/n\mathbb{Z}$. These three functions are simple to code so they will not be given. Also, since the functions SQUARES and FOURPOWERS are only used once each, there is not much need to program them efficiently.

The two algorithms that we give both need the same subalgorithm that we will call SOLCHECK(e_2,e_3,b_1,b_2,2^q,S,R). SOLCHECK checks if the equation system has a solution in $\mathbb{Z}/2^q\mathbb{Z}$ for the given quadruple (e_2,e_3,b_1,b_2). S being the subset generated by SQUARES(2^q) and R the one generated by FOURPOWERS(2^q).

Algorithm 2 Checks the existence of a non trivial solution for Equation System (3.1.1) in $\mathbb{Z}/2^q\mathbb{Z}$ for the given e_2,e_3,b_1,b_2.

```
procedure SOLCHECK($e_2$,$e_3$,$b_1$,$b_2$,$2^q$,$S$,$R$)
    for $Z_1 \in S$ do
        for $Z_2 \in S$ do
            for $D \in R$ do
                if $b_1Z_1 - b_2Z_2 \equiv_{2^q} e_2D$ then
                    for $Z_3 \in S$ do
                        if $GCD(Z_1,Z_2,Z_3,D) \equiv_2 1$ then
                            if $b_1Z_1 - b_1b_2Z_3 \equiv_{2^q} e_3D$ then
                                return True
    return False
```

This algorithm is pretty much looking at every possible solution by brute force with two small tricks that save a considerable amount of time. The first one is the change of variables $Z_i = z_i^2$ and $D = d^2$. By taking these new variables and limiting their domain to the subset of squares S, we do not need to calculate the square of our variables every time. The second trick is to divide the equation system by $\overline{d}$ to always guarantee that d is a power of 4 and not have to do most of the cases.

With this subalgorithm, we can do the sufficiency algorithm.

Algorithm 3 Verification that the set of conditions C are sufficient for a solution in $\mathbb{Z}/2^q\mathbb{Z}$ when $v_2(e_2) = w_2$ and $v_2(e_3) = w_3$.

```
procedure SUFFICIENT($C$, $2^q$, $w_2$, $w_3$)
    $S \leftarrow$ SQUARES($2^q$)
    $R \leftarrow$ FOURPOWERS($2^q$)
    for $e_2$ from $2^{q-1}+1$ to $2^{q-1}$ do
        if $v_2(e_2) = w_2$ then
            for $e_3$ from $2^{q-1}+1$ to $2^{q-1}$ do
                if $v_2(e_3) = w_3$ then
                    for $b_1$ from $2^{q-1}+1$ to $2^{q-1}$ do
                        if $b_1 \not\equiv_4 0$ then
                            for $b_2$ from $2^{q-1}+1$ to $2^{q-1}$ do
                                if $b_2 \not\equiv_4 0$ then
                                    if $C(e_2,e_3,b_1,b_2)$ = True then
                                        if SOLCHECK($e_2$,$e_3$,$b_1$,$b_2$,$2^q$,$S$,$R$) = False then
                                            return False
    return True
```

This algorithm is also by brute force. It simply checks if every quadruple (e_2,e_3,b_1,b_2) respecting our conditions also has solution.

The necessity algorithm is very similar:

Algorithm 4 Verification that the set of conditions C are necessary for a solution in $\mathbb{Z}/2^q\mathbb{Z}$ when $v_2(e_2) = w_2$ and $v_2(e_3) = w_3$.

```
procedure NECESSARY($C$, $2^q$, $w_2$, $w_3$)
    $S \leftarrow$ SQUARES($2^q$)
    $R \leftarrow$ FOURPOWERS($2^q$)
    for $e_2$ from $2^{q-1}+1$ to $2^{q-1}$ do
        if $v_2(e_2) = w_2$ then
            for $e_3$ from $2^{q-1}+1$ to $2^{q-1}$ do
                if $v_2(e_3) = w_3$ then
                    for $b_1$ from $2^{q-1}+1$ to $2^{q-1}$ do
                        if $b_1 \not\equiv_4 0$ then
                            for $b_2$ from $2^{q-1}+1$ to $2^{q-1}$ do
                                if $b_2 \not\equiv_4 0$ then
                                    if $C(e_2,e_3,b_1,b_2)$ = False then
                                        $m \leftarrow 4$
                                        GoOn $\leftarrow$ True
                                        while $m \leq 2^q$ and GoOn do
                                            if SOLCHECK($e_2,e_3,b_1,b_2,2^q,S,R$) = True then
                                                $m \leftarrow 2m$
                                            else
                                                GoOn $\leftarrow$ False
                                        if GoOn then
                                            return False
    return True
```

The main difference here is that the algorithm studies the quadruples (e_2,e_3,b_1,b_2) not respecting the conditions instead of those who do. We also have added a simple trick. Instead of directly verifying that there is no solution in $\mathbb{Z}/2^q\mathbb{Z}$, we verify that there is no solution in $\mathbb{Z}/2^r\mathbb{Z}$ for $r = 2$ and then increase r by one at a time until we reach $\mathbb{Z}/2^q\mathbb{Z}$. It saves time in most cases since the majority of quadruples not having a solution in $\mathbb{Z}/2^q\mathbb{Z}$ also do not have solutions in $\mathbb{Z}/2^r\mathbb{Z}$ for some $r < q$. Since verifying the non-existence of a solution in $\mathbb{Z}/2^r\mathbb{Z}$ is a lot faster that in $\mathbb{Z}/2^q\mathbb{Z}$, this saves us a considerable amount of time when we add up all cases.

Références bibliographiques

[BWP61] B. Boncompagni, M.F. Woepcke, and Biblioteca Provinciale. *Recherches sur plusieurs ouvrages de Leonard de Pise decouverts et publiés par M. le prince Balthasar Boncompagni.* 1861.

[Fuj02] Masahiko Fujiwara. Some properties of θ-congruent numbers. *Natur. Sci. Rep. Ochanomizu Univ.*, 52(2):1–8, 2002.

[GLN18] Vincent Girard, Matilde N. Lalín, and Sivasankar C. Nair. Families of non-θ-congruent numbers with arbitrarily many prime factors. *Colloq. Math.*, 152(2):255–271, 2018.

[Har77] Robin Hartshorne. *Algebraic geometry.* Springer-Verlag, New York-Heidelberg, 1977. Graduate Texts in Mathematics, No. 52.

[HB94] D. R. Heath-Brown. The size of Selmer groups for the congruent number problem. II. *Invent. Math.*, 118(2):331–370, 1994. With an appendix by P. Monsky.

[Isk96] Boris Iskra. Non-congruent numbers with arbitrarily many prime factors congruent to 3 modulo 8. *Proc. Japan Acad. Ser. A Math. Sci.*, 72(7):168–169, 1996.

[Kob93] Neal Koblitz. *Introduction to elliptic curves and modular forms*, volume 97 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1993.

[Leg08] A. M. (Adrien Marie) Legendre. *Essai sur la théorie des nombres.* Paris :Duprat„ 1808. https://www.biodiversitylibrary.org/bibliography/18546 — Master microform held by: Readex. — Continued by: Landmarks II.

[LT00] Delang Li and Ye Tian. On the Birch-Swinnerton-Dyer conjecture of elliptic curves $E_D\colon y^2 = x^3 - D^2x$. *Acta Math. Sin. (Engl. Ser.)*, 16(2):229–236, 2000.

[Maz77] B. Mazur. Modular curves and the Eisenstein ideal. *Inst. Hautes Études Sci. Publ. Math.*, (47):33–186 (1978), 1977. With an appendix by Mazur and M. Rapoport.

[Maz78] B. Mazur. Rational isogenies of prime degree (with an appendix by D. Goldfeld). *Invent. Math.*, 44(2):129–162, 1978.

[Mok20] Youcef Mokrani. Adaptation of Monsky matrices for θ-congruent numbers. *Int. J. Number Theory*, 16(2):377–396, 2020.

[RSY13] Lindsey Reinholz, Blair K. Spearman, and Qiduan Yang. Families of non-congruent numbers with arbitrarily many prime factors. *J. Number Theory*, 133(1):318–327, 2013.

[RSY15] Lindsey Reinholz, Blair K. Spearman, and Qiduan Yang. On the prime factors of non-congruent numbers. *Colloq. Math.*, 138(2):271–282, 2015.

[RSY18] Lindsey Reinholz, Blair K. Spearman, and Qiduan Yang. An extension theorem for generating new families of non-congruent numbers. *Funct. Approx. Comment. Math.*, 58(1):69–77, 2018.

[Ser91] P. Serf. Congruent numbers and elliptic curves. In *Computational number theory (Debrecen, 1989)*, pages 227–238. de Gruyter, Berlin, 1991.

[Sil09] Joseph H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics*. Springer, Dordrecht, second edition, 2009.

[Tun83] J. B. Tunnell. A classical Diophantine problem and modular forms of weight 3/2. *Invent. Math.*, 72(2):323–334, 1983.

[Wei29] André Weil. L'arithmétique sur les courbes algébriques. *Acta Math.*, 52:281–315, 1929.

[Yos01] Shin-ichi Yoshida. Some variants of the congruent number problem. I. *Kyushu J. Math.*, 55(2):387–404, 2001.

[Yos02] Shin-ichi Yoshida. Some variants of the congruent number problem. II. *Kyushu J. Math.*, 56(1):147–165, 2002.

[Zag90] D. Zagier. Elliptische Kurven: Fortschritte und Anwendungen. *Jahresber. Deutsch. Math.-Verein.*, 92(2):58–76, 1990.