The Generation of Families of Non-congruent Numbers with Arbitrarily Many Prime Factors

by

Lindsey Kayla Reinholz

B.Sc., The University of British Columbia, 2011
M.Sc., The University of British Columbia, 2013

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

DOCTOR OF PHILOSOPHY

in

The College of Graduate Studies

(Mathematics)

THE UNIVERSITY OF BRITISH COLUMBIA

(Okanagan)

October 2019

The following individuals certify that they have read, and recommend to the College of Graduate Studies for acceptance, a thesis/dissertation entitled:

The Generation of Families of Non-congruent Numbers with Arbitrarily Many Prime Factors

submitted by Lindsey Kayla Reinholz in partial fulfilment of the requirements of the degree of Doctor of Philosophy

Dr. Qiduan Yang, Department of Computer Science, Mathematics, Physics, and Statistics
Co-supervisor

Dr. Sylvie Desjardins, Department of Computer Science, Mathematics, Physics, and Statistics
Supervisory Committee Member

Dr. Shawn Wang, Department of Computer Science, Mathematics, Physics, and Statistics
Supervisory Committee Member

Dr. Karen Perry, Department of Chemistry
University Examiner

Dr. Yang Zhang, Department of Mathematics, University of Manitoba
External Examiner

Abstract

A congruent number n is a positive integer that is equal to the area of a right triangle with rational side lengths. Positive integers for which such a representation does not exist are called non-congruent numbers. Equivalently, n is non-congruent if and only if the arithmetic rank of the cubic curve

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

known as a congruent number elliptic curve, is zero. Determining whether or not a given positive integer is congruent in a finite number of steps is a problem of significant interest in the field of pure mathematics. Although a complete solution to this classical problem has yet to be discovered, progress has been made in describing particular families of congruent and non-congruent numbers. The classification of numbers into such families is often done by imposing conditions on the prime divisors of the numbers and on the Legendre symbols relating the primes.

This thesis focuses on the generation of both odd and even non-congruent numbers. We present a new family of even non-congruent numbers that are a product of arbitrarily many distinct primes; these non-congruent numbers have at least one prime factor in each odd congruence class modulo eight. Our main contribution is the development of a general approach for constructing families of non-congruent numbers. We show that existing families of non-congruent numbers can be extended by working over the finite field with two elements and using a formula by Monsky for computing the 2-Selmer rank of congruent number elliptic curves. The new non-congruent numbers are produced by multiplying known non-congruent numbers, corresponding to congruent number elliptic curves with 2-Selmer rank of zero, by arbitrarily many suitable primes. This novel technique allows an infinite collection of non-congruent numbers to be generated, including both odd and even non-congruent numbers with arbitrarily many distinct prime divisors in each odd congruence class modulo eight. Our results are illustrated by numerous numerical examples.

Lay Summary

This thesis studies a particular set of numbers known as non-congruent numbers. Every positive integer can be classified as either a congruent number or a non-congruent number. A congruent number is a positive integer that is equal to the area of a right-angled triangle with side lengths that are rational numbers. If such a representation does not exist, then the integer is called a non-congruent number. The classification of positive integers as either congruent or non-congruent is an open problem that has been studied for centuries.

In this thesis, we present criteria for generating non-congruent numbers that have arbitrarily many prime divisors. Our main contribution is a new method for constructing non-congruent numbers. We show that when existing non-congruent numbers with a specific property are multiplied by arbitrarily many suitable primes, infinitely many new non-congruent numbers are produced. Our results are illustrated by a collection of numerical examples.

Preface

My achievements as a graduate student would not have been possible without the support, guidance, and encouragement I received from my supervisor, Dr. Blair Spearman, who passed away on October 1, 2017. Though Dr. Spearman unfortunately did not have the opportunity to read my thesis or to participate in my doctoral defence, I consider him to be my Ph.D. supervisor. Dr. Spearman's recognition of my research potential is what lead me to pursue graduate studies, and it is an honour to be able to complete my doctoral degree in his memory.

The research work presented in this thesis is based on the following four papers.

Published:

[41] L. Reinholz, B. K. Spearman, and Q. Yang. *An extension theorem for generating new families of non-congruent numbers*, Funct. Approx. Comment. Math., 58 (2018), pp. 69-77.

[42] L. Reinholz, B. K. Spearman, and Q. Yang. *Families of even non-congruent numbers with prime factors in each odd congruence class modulo eight*, Int. J. Number Theory, 14 (2018), pp. 669-692.

Submitted:

[43] L. Reinholz and Q. Yang. *On the extension of even families of non-congruent numbers.*

[44] L. Reinholz and Q. Yang. *On the generation of odd non-congruent numbers with arbitrarily many prime factors.*

Specifically, Chapter 4 focuses on a theorem from [42]; Chapter 5 is based on the work in [41] and [44]; and Chapter 6 is comprised of results presented in [42] and [43].

For each of the aforementioned multi-authored papers, I developed and proved all of the theorems, and I wrote each of the manuscripts. My collaborators provided guidance and constructive criticism throughout the research and publication process.

Table of Contents

List of Tables

List of Figures

Glossary of Notation and Symbols

$\mathbb{Z}$	Set of integers, $\{\ldots,-2,-1,0,1,2,\ldots\}$	**p. 3**
$\mathbb{N}$	Set of natural numbers, $\{0,1,2,\ldots\}$	**p. 18**
$\mathbb{N}^+$	Set of natural numbers excluding zero, $\{1,2,3\ldots\}$	**p. 2**
$\mathbb{R}$	Set of real numbers	**p. 9**
$\mathbb{Q}^*$	Multiplicative group of nonzero rational numbers	**p. 26**
$\mathbb{Q}^{*2}$	Group of squares of elements of $\mathbb{Q}^*$	**p. 26**
$\mathbb{Q}^*/\mathbb{Q}^{*2}$	Quotient group of square-free, nonzero rational numbers	**p. 26**
$\mathbb{Q}_p$	Field of p-adic numbers	**p. 9**
$\mathbb{Z}_n$	Cyclic group of order n, $\{0,1,2,\ldots,n-1\}$	**p. 20**
$\mathbb{Z}_{p_i^{\nu_i}}$	The cyclic group with prime-power order	**p. 5**
$\mathbb{Z}_{n_1}\oplus\mathbb{Z}_{n_2}\oplus\cdots\oplus\mathbb{Z}_{n_w}$	Direct sum of cyclic groups	**p. 5**
$\mathbb{Z}_{n_1}\times\mathbb{Z}_{n_2}\times\cdots\times\mathbb{Z}_{n_w}$	Direct product of cyclic groups	**p. 20**
$\mathbb{F}_q$	Finite field with q elements	**p. 20**
$\lvert S\rvert$	Number of elements in the set S	**p. 3**
$\langle S,*\rangle$	Binary algebraic structure with non-empty set S and binary operation $*$	**p. 5**
$S\cong S'$	Isomorphic structures	**p. 18**
$\ker(\phi)$	Kernel of the homomorphism ϕ	**p. 6**
G/N	Quotient group	**p. 26**
$\mathrm{Im}(b)$	Image of the homomorphism b	**p. 6**
(a,b)	Greatest common divisor of a and b	**p. 6**
$a\mid b$	a divides b	**p. 7**
$a\nmid b$	a does not divide b	**p. 7**
$a\equiv b \pmod{m}$	a is congruent to b modulo m	**p. 7**

$\left(\dfrac{a}{p}\right)$	Legendre symbol	**p. 8**
$v_p(x)$	p-adic valuation of x	**p. 9**
$\mathbf{I_n}$	Identity matrix of order n	**p. 10**
$\mathbf{0}$	$m \times n$ zero matrix	**p. 10**
$\mathbf{0_n}$	Zero matrix of order n	**p. 10**
$\mathbf{A}^T$	Transpose of the matrix $\mathbf{A}$	**p. 10**
$\mathbf{A}^{-1}$	Inverse of the matrix $\mathbf{A}$	**p. 11**
$\mathrm{rank}(\mathbf{A})$	Rank of the matrix $\mathbf{A}$	**p. 10**
$\det(\mathbf{A})$	Determinant of the matrix $\mathbf{A}$	**p. 10**
C_x	Column x in a matrix	**p. 10**
R_x	Row x in a matrix	**p. 10**
$C_x \longrightarrow C_x + C_y$	Replacement of column C_x by the sum of columns C_x and C_y	**p. 10**
$C_x \longleftrightarrow C_y$	Interchange of columns C_x and C_y	**p. 10**
$R_x \longrightarrow R_x + R_y$	Replacement of row R_x by the sum of rows R_x and R_y	**p. 34**
$R_x \longleftrightarrow R_y$	Interchange of rows R_x and R_y	**p. 36**
E_n	Congruent number elliptic curve $y^2 = x^3 - n^2x$	**p. 2**
$\mathbb{P}^2$	Projective plane	**p. 12**
$[X : Y : Z]$	Homogeneous coordinates or projective coordinates for a point in the projective plane	**p. 12**
$\mathscr{O}$	Point at infinity on an elliptic curve	**p. 12**
$P + Q$	Addition of the points P and Q on an elliptic curve	**p. 15**
$E(K)$	Group of K-rational points on the elliptic curve E over the field K	**p. 15**
$\mathscr{T}$	Torsion subgroup of the elliptic curve E	**p. 18**
$\mathscr{T}_n$	Torsion subgroup of the elliptic curve E_n	**p. 22**
$r(n)$	Arithmetic rank or Mordell-Weil rank of the elliptic curve E_n	**p. 27**
$E_n/\mathbb{Q}$	Elliptic curve E_n over the field $\mathbb{Q}$	**p. 28**
$\mathrm{Sel}_2(E_n/\mathbb{Q})$	2-Selmer group of $E_n/\mathbb{Q}$	**p. 28**
$\Sha(E_n/\mathbb{Q})[2]$	Shafarevich-Tate group of $E_n/\mathbb{Q}$	**p. 28**
$s(n)$	2-Selmer rank of the elliptic curve E_n	**p. 29**
$S\backslash T$	Set S excluding the elements in the set T	**p. 26**
∞	Infinite prime	**p. 26**

$M_{\mathbb{Q}}$	Set of all places of the field $\mathbb{Q}$, $\{\infty, 2, 3, \ldots\}$	**p. 26**
$\emptyset$	Empty set	**p. 42**

Acknowledgements

First and foremost, I would like to express my deepest gratitude to my late supervisor, Dr. Blair Spearman. I had the pleasure of working under his supervision for eight years and am incredibly thankful for the guidance, encouragement, patience, and unfailing support that he showed me throughout my educational journey. His recognition of and confidence in my potential as a researcher are ultimately what lead me to pursue graduate studies. I am immensely grateful for all of the time and effort that he so generously contributed to helping me achieve my academic and career goals.

I would like to sincerely thank my co-supervisor Dr. Qiduan Yang. His constructive criticism and broad knowledge have proved invaluable to my research work, and I am incredibly thankful for the constant support and encouragement he has given me throughout my graduate studies. I am also immensely grateful that after tragic circumstances arose, he so kindly agreed to oversee the completion of my doctoral degree.

In addition, I would like to express my heartfelt thanks to my committee members, Dr. Sylvie Desjardins and Dr. Shawn Wang. During my time as a graduate student, they have been dedicated mentors who have provided me with guidance, advice, and support. I truly appreciate the many contributions they each have made to help me successfully complete my education and achieve my career goal.

I would like to extend my gratitude to the members of the Department of Computer Science, Mathematics, Physics, and Statistics at UBC Okanagan. In particular, I wish to thank my colleagues Dr. Chad Davis, Dr. Paul Lee, Stephen Brown, and Jeewon Yoo for their advice, support, and friendship. Special thanks also goes to Hiroko Nakahara for her encouragement, and for the valuable experience and skills I gained while working under her supervision.

I wish to acknowledge both UBC Okanagan and the Natural Sciences and Engineering Research Council of Canada for their financial support throughout my doctoral studies.

Finally, I would like to sincerely thank my family and friends for their encouragement, love, and understanding throughout every step of my education. This journey has been immensely challenging at times, and I am forever grateful to my parents, brothers, and Jonathon for the sacrifices they have made to ensure my success, and for the unconditional love and support they have shown me; this accomplishment would not have been possible without them.

Dedication

In memory of Dr. Blair Spearman. I never had the opportunity to fully thank you for everything you so selflessly did for me over the eight years I knew you. Your recognition of my research potential and encouragement to pursue graduate studies changed my educational and career paths. You were an incredible mentor and a dedicated teacher, who positively influenced so many lives. You are truly missed.

Chapter 1

Introduction

The classification of positive integers as either congruent or non-congruent numbers is an unsolved problem in the fields of algebra and number theory with an extensive history. There exist several equivalent definitions of congruent numbers, but perhaps the most well-known is the one that relates congruent numbers to right-angled triangles.

Definition 1.1. A positive integer n is a *congruent number* if it is equal to the area of a right triangle with rational sides. Otherwise n is said to be a *non-congruent number*.

This means that n is a congruent number if there exist rational numbers a, b, and c such that

$$a^2 + b^2 = c^2 \qquad \text{and} \qquad n = \frac{ab}{2}. \tag{1.1}$$

The positive integer six is an example of a congruent number.

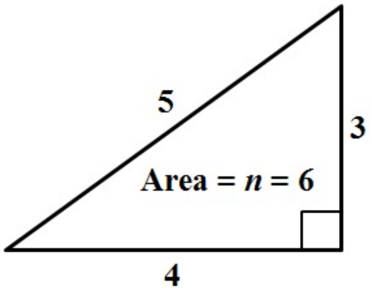


Figure 1.1: The congruent number six is equal to the area of a right triangle with rational side lengths.

There are infinitely many positive integers that cannot be written as the area of a right triangle with rational side lengths, including the numbers one, two, three, and four; these numbers are non-congruent. A list of all congruent numbers less than 10,000 can be found in [35].

By inspecting the pair of equations in (1.1), it is clear that scaling the side lengths of a triangle changes its area by a factor of a square. Therefore, if n is a congruent number, so too is nm^2, where $m \in \mathbb{N}^+$. As a result, it is a common practice to only consider square-free positive integers when studying congruent numbers.

The search for a general solution to the problem that involves determining whether a given number is congruent has fascinated mathematicians for centuries. Although the study of congruent numbers has its origins in ancient Greece, the first systematic discussion of the congruent number problem appears in a pair of Arab manuscripts from the tenth century [5, 8, 25, 29, 56, 60]. Since that time, notable contributions to the field of congruent numbers have been made by many well-known mathematicians, including Fibonacci, Euler, and Fermat [5, 8]. In his book *Liber Quadratorum* (1225), Fibonacci verified that both five and seven are congruent numbers [5, 8, 32, 56]. He also conjectured that perfect squares cannot be congruent numbers, or equivalently that the integer one is non-congruent. Fibonacci's conjecture remained unproven for four centuries, and ultimately led to Fermat's significant discovery of the method of infinite descent. For a proof that one is a non-congruent number using the method of infinite descent, see [5].

In the twentieth century, congruent numbers were shown to be related to a special type of cubic algebraic curve known as an elliptic curve [25]. The relationship between elliptic curves and congruent numbers is summarized by the following lemma.

Lemma 1.2. *A positive integer n is a congruent number if and only if the rank of the elliptic curve*

$$E_n : y^2 = x^3 - n^2x = x(x-n)(x+n)$$

is positive. Otherwise, n is a non-congruent number. In other words, n is a non-congruent number if and only if the rank of E_n is zero.

A proof of this lemma can be found in Section 9 of Chapter I in [25]. Also, note that the properties of and theory governing elliptic curves and their rank will be discussed in detail in Chapter 3.

In his groundbreaking paper published in 1983, Tunnell used the theory of elliptic curves to state and prove an elegant theorem that provides a simple, but complete, characterization of congruent numbers [5, 25, 29, 46, 56, 57].

Theorem 1.3 (**Tunnell's Theorem**). *Let n be a square-free congruent number and define*

$$\begin{aligned} A_n &= |\{(x,y,z) \in \mathbb{Z}^3 | n = 2x^2 + y^2 + 32z^2\}|, \\ B_n &= |\{(x,y,z) \in \mathbb{Z}^3 | n = 2x^2 + y^2 + 8z^2\}|, \\ C_n &= |\{(x,y,z) \in \mathbb{Z}^3 | n = 8x^2 + 2y^2 + 64z^2\}|, \\ D_n &= |\{(x,y,z) \in \mathbb{Z}^3 | n = 8x^2 + 2y^2 + 16z^2\}|. \end{aligned}$$

Then

$$\begin{cases} B_n = 2A_n \text{ if } n \text{ is odd,} \\ D_n = 2C_n \text{ if } n \text{ is even.} \end{cases}$$

If the Birch and Swinnerton-Dyer conjecture holds for elliptic curves of the form $y^2 = x^3 - n^2x$ then, conversely, these equalities imply that n is a congruent number.

Proof. See Tunnell's paper [57]. Koblitz's book [25] is also an excellent resource that provides a comprehensive discussion of Tunnell's theorem and the extensive collection of theory required to complete its challenging proof. □

Unfortunately, Tunnell's theorem does not entirely resolve the congruent number problem, as one direction of it relies upon the Birch and Swinnerton-Dyer conjecture, which is currently unproven. This famous conjecture is one of the seven Millennium Prize Problems posed by the Clay Mathematics Institute. Because the results in this thesis do not depend upon the Birch and Swinnerton-Dyer conjecture, we do not provide additional information in this dissertation. A thorough discussion of the conjecture is given in an article by Andrew Wiles on the website of the Clay Mathematics Institute [60].

A comprehensive overview of the history of the congruent number problem and the progress that has been made towards its solution can be found in [5, 8, 56].

1.1 The Goal of the Thesis

Because it is difficult to find a complete solution to the congruent number problem, mathematicians focus on describing and generating particular families of congruent and non-congruent numbers. Such families can be obtained by imposing certain conditions on their prime factors and the values of the Legendre symbols relating the primes; see [2, 6, 11–13, 15–17, 24, 27, 28, 36, 37, 39, 40, 49, 58].

The goal of this thesis is to construct new families of odd non-congruent numbers and even non-congruent numbers with arbitrarily many distinct prime factors. Of specific interest is the generation of families of non-congruent numbers with prime factors belonging to each odd congruence class modulo eight, and the development of methods that allow known non-congruent numbers to be extended to produce new families of non-congruent numbers.

1.2 The Structure of the Thesis

This section provides a brief overview of the layout and main contributions of the research presented within this dissertation.

Chapter 2 contains a collection of notation and basic theory from the fields of algebra, number theory, and linear algebra. Chapter 3 covers known results on elliptic curves with an emphasis on their connection to the congruent number problem. We also discuss Monsky's formula for the 2-Selmer rank of E_n.

Our main contributions are presented in Chapters 4, 5, and 6. Chapter 4 focuses on generating a new family of even non-congruent numbers with arbitrarily many distinct prime divisors; these non-congruent numbers have prime factors in each odd congruence class modulo eight. Chapters 5 and 6 introduce our new general extension technique for constructing families of non-congruent numbers from other known families of non-congruent numbers. Chapter 5 focuses on the generation of odd non-congruent numbers, whereas Chapter 6 is dedicated to the construction of even non-congruent numbers. In each of these chapters, a detailed proof of the technique for generating non-congruent numbers is presented along with a collection of numerical examples that illustrate how the method can be applied.

Finally, we summarize our research contributions and discuss future research avenues in Chapter 7.

Chapter 2

Preliminary Information

In this chapter, we present a collection of notation, terminology, and theory from algebra, number theory, and linear algebra.

2.1 Algebra Preliminaries

We begin by recalling some definitions and theorems from the field of algebra. The theory in this section closely follows that in [14] and can be found in most introductory algebra texts.

Definition 2.1. Let G be a group and let $a \in G$. The element *a generates* the group G and is referred to as a *generator* of G if $G = \{a^n | n \in \mathbb{Z}\ \} = \langle a \rangle$. If this is the case, then G is said to be *cyclic*.

Definition 2.2. An abelian group $\langle G, + \rangle$ is *finitely generated* if it contains a finite set of elements $\{g_1, g_2, \ldots, g_n\}$ such that every element $g \in G$ can be written as

$$g = a_1 g_1 + a_2 g_2 + \cdots + a_n g_n,$$

where $a_1, a_2, \ldots, a_n \in \mathbb{Z}$.

We now state an important result that completely describes the structure of all finitely generated abelian groups [14, Theorem 11.12].

Theorem 2.3 (Fundamental Theorem of Finitely Generated Abelian Groups). *Every finitely generated abelian group is isomorphic to a direct sum of cyclic groups*

$$\mathbb{Z}_{p_1^{\nu_1}} \oplus \mathbb{Z}_{p_2^{\nu_2}} \oplus \cdots \oplus \mathbb{Z}_{p_\omega^{\nu_\omega}} \oplus \underbrace{\mathbb{Z} \oplus \mathbb{Z} \oplus \cdots \oplus \mathbb{Z}}_{r\ copies},$$

where the p_i are primes that are not necessarily distinct, $\nu_i \in \mathbb{N}^+$ for all $i \in [1, \omega]$, and $r \in \mathbb{N}$.

The following theorem describes the relationship between the order of a finitely generated abelian group and its subgroups.

Theorem 2.4. *If m divides the order of a finite abelian group G, then G has a subgroup of order m.*

Definition 2.5. A *field* is an integral domain D in which every nonzero element of D has a multiplicative inverse in D.

Definition 2.6. The *characteristic* of a field K is the least positive integer n such that $n \cdot a = 0$ for all $a \in K$. If no such positive integer exists, then K has characteristic zero.

Definition 2.7. A sequence

$$G_0 \xrightarrow{\delta_1} G_1 \xrightarrow{\delta_2} G_2 \xrightarrow{\delta_3} \cdots \xrightarrow{\delta_n} G_n$$

of groups G_k and homomorphisms δ_k is an *exact sequence* if

$$\mathrm{Im}(\delta_k) = \ker(\delta_{k+1}).$$

An exact sequence of the form

$$0 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 0$$

is called a *short exact sequence* if the map f is injective, the map g is surjective, and $\mathrm{Im}(f) = \ker(g)$.

2.2 Number Theory Preliminaries

This section provides a collection of definitions and theorems from the field of number theory. Wherever not explicitly specified, the notation follows that in [46].

Definition 2.8. The *parity* of an integer defines the value as either even or odd.

Definition 2.9. The *greatest common divisor* of two integers a and b, which are not both equal to zero, is the largest positive integer that divides both a and b. The greatest common divisor of a and b is denoted by (a, b), and $(0, 0)$ is defined to be zero.

Definition 2.10. Consider the set of integers $A = \{a_1, a_2, \ldots, a_n\}$ and let $a_i, a_j \in A$ with $i \neq j$. The integers a_i and a_j are *relatively prime* if $(a_i, a_j) = 1$. The integers $a_1, a_2, \ldots, a_n$ are said to be *pairwise relatively prime*, if each pair of integers from the set A is relatively prime.

Note that for two integers a and b, the notation $a|b$ denotes that a divides b, whereas $a \nmid b$ indicates that a does not divide b.

Definition 2.11. Let m be a positive integer. If a and b are integers, then a is *congruent to b modulo m* if $m|(a-b)$. To denote that a is congruent to b modulo m, we write $a \equiv b \pmod{m}$. If $m \nmid (a-b)$, then a and b are *incongruent modulo m*, which is written as $a \not\equiv b \pmod{m}$. The integer m is called the *modulus* of the congruence.

Definition 2.12. Let $a \in \mathbb{Z}$ and $m \in \mathbb{N}^+$. The *congruence class of a modulo m* is the set of all integers that are congruent to a modulo m.

For example, there are four congruence classes modulo four. The first congruence class contains all integers congruent to 0 (mod 4), the second is comprised of integers congruent to 1 (mod 4), the third contains the integers congruent to 2 (mod 4), and the fourth consists of integers congruent to 3 (mod 4). The integers belonging to a particular one of these congruence classes have the form $4k+i$, where $k \in \mathbb{Z}$ and i is equal to either 0, 1, 2, or 3.

The following theorem, known as the Chinese Remainder Theorem, provides a method for solving systems of simultaneous congruences with only one unknown, but different moduli [46, Theorem 4.12].

Theorem 2.13 (**Chinese Remainder Theorem**). *If $m_1, m_2, \ldots, m_s$ are pairwise relatively prime positive integers, then the system of congruences*

$$\begin{aligned} x &\equiv a_1 \pmod{m_1}, \\ x &\equiv a_2 \pmod{m_2}, \\ &\vdots \\ x &\equiv a_s \pmod{m_s}, \end{aligned}$$

has a unique solution modulo $M = m_1 m_2 \cdots m_s$.

The proof of Theorem 2.13, along with numerical examples illustrating its application, can be found in [46].

Fermat's little theorem, which we state next, describes an important congruence property for the pth powers of integers modulo p, where p is a prime [46, Theorem 6.3].

Theorem 2.14 (**Fermat's Little Theorem**). *If p is a prime and b is a positive integer with $p \nmid b$, then $b^{p-1} \equiv 1 \pmod{p}$.*

Next, we provide the definition of quadratic residues and quadratic nonresidues to motivate our discussion of Legendre symbols.

Definition 2.15. If m is a positive integer, we say that the integer b is a *quadratic residue* of m if $(b, m) = 1$ and the congruence $x^2 \equiv b \pmod{m}$ has a solution. If this congruence does not have a solution, then we say that b is a *quadratic nonresidue* of m.

The concept of a quadratic residue can be used to define a multiplicative function known as a Legendre symbol.

Definition 2.16. Let p be an odd prime and a be an integer not divisible by p. The *Legendre symbol* $\left(\frac{a}{p}\right)$ is defined by

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } a \text{ is a quadratic residue of } p, \\ -1 & \text{if } a \text{ is a quadratic nonresidue of } p. \end{cases}$$

Legendre symbols will be used extensively throughout this thesis. We summarize some of their useful properties in Theorems 2.17, 2.18, and 2.19 [46, Theorems 11.4, 11.5, 11.6 & 11.7].

Theorem 2.17. *Let p be an odd prime and a and b be integers not divisible by p. Then*

1) *if* $a \equiv b \pmod{p}$, *then* $\left(\dfrac{a}{p}\right) = \left(\dfrac{b}{p}\right)$,

2) $\left(\dfrac{a}{p}\right)\left(\dfrac{b}{p}\right) = \left(\dfrac{ab}{p}\right)$,

3) $\left(\dfrac{a^2}{p}\right) = 1$.

Theorem 2.18 (The Law of Quadratic Reciprocity). *If p and q are distinct odd primes, then*

$$\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right)(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}.$$

Theorem 2.19 (The First and Second Supplements to the Law of Quadratic Reciprocity). *If p is an odd prime, then*

1) $\left(\dfrac{-1}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1 \pmod{4}, \\ -1 & \text{if } p \equiv 3 \pmod{4}, \end{cases}$

2) $\left(\dfrac{2}{p}\right) = \begin{cases} 1 & \text{if } p \equiv \pm 1 \pmod{8}, \\ -1 & \text{if } p \equiv \pm 3 \pmod{8}. \end{cases}$

We now state a pair of important and well-known theorems; the first pertains to primes in arithmetic progressions [46, Theorem 3.3], [50, Chapter VI], and the second discusses how primes are the multiplicative building blocks of all integers [46, Theorem 3.15].

Theorem 2.20 (**Dirichlet's Theorem on Primes in Arithmetic Progressions**)**.** *Suppose that a and b are relatively prime positive integers. Then there are infinitely many primes in the arithmetic progression $an + b$, where $n \in \mathbb{N}^+$.*

Theorem 2.21 (**The Fundamental Theorem of Arithmetic**)**.** *Every positive integer greater than one can be written as a product of primes, and this representation is unique up to the order of the prime factors.*

We also recall an elementary definition from p-adic number theory [18].

Definition 2.22. Let p be a prime number and x be a nonzero rational number. If

$$x = p^\alpha \cdot \frac{a}{b}$$

where $p \nmid ab$, then the *p-adic valuation*, $v_p(x)$, of x is

$$v_p(x) = \alpha.$$

It is a well-known fact that if a polynomial with rational coefficients has roots in $\mathbb{Q}$, then it also has roots in $\mathbb{R}$ and in $\mathbb{Q}_p$ for every prime $p \geq 2$. Therefore, a polynomial has no rational roots when there is a prime $p \leq \infty$ for which it does not have any p-adic roots. This leads us to the following definition [18].

Definition 2.23. A polynomial equation with rational coefficients is said to have *local solutions* if it has roots in $\mathbb{R}$ and in $\mathbb{Q}_p$ for every prime $p \geq 2$. If the polynomial equation has roots over $\mathbb{Q}$, these are called *global solutions.*

Thus, a polynomial equation with global solutions also has local solutions for every prime. We now state an important principle by Hasse, known as the local-global principle or the Hasse principle [18, Section 3.5].

Principle 2.24 (**Hasse Principle**)**.** *The existence or non-existence of global solutions of a Diophantine equation can be detected by studying the local solutions of the equation.*

In other words, an equation has a solution over $\mathbb{Q}$ if and only if it has solutions over $\mathbb{R}$ and $\mathbb{Q}_p$ for all primes $p \geq 2$. The Hasse-Minkowski theorem states that the Hasse principle holds for quadratic forms in m variables with coefficients in the field K [18, 50]. Unfortunately, the Hasse principle does not always hold true, as many equations are locally solvable everywhere but fail to have global solutions. For example, Selmer proved that the equation $3x^3 + 4y^3 + 5y^3 = 0$ has a nontrivial solution in the real numbers and in all p-adic fields, but it does not have a nontrivial rational solution [48]. This shows that the Hasse-Minkowski theorem cannot be extended to cubic forms.

2.3 Linear Algebra Preliminaries

In this section, we discuss various notation, terminology, and results from linear algebra.

We denote the identity matrix of order n by $\mathbf{I_n}$, the zero matrix of order n by $\mathbf{0_n}$, and any non-square zero matrix by $\mathbf{0}$.

Let $\mathbf{A} = [a_{ij}]$ be an $m \times n$ matrix. The transpose of $\mathbf{A}$ is denoted by $\mathbf{A}^T$. We introduce the following notation to describe elementary row and column operations within a matrix $\mathbf{A}$.

Notation: For a given matrix $\mathbf{A}$, let C_x denote column x and R_x denote row x, where $x \in \mathbb{N}^+$. Then

$$C_x \longrightarrow C_x + C_y$$

is used to represent the replacement of column C_x by the sum of columns C_x and C_y. Finally, we denote the interchange of columns C_x and C_y by

$$C_x \longleftrightarrow C_y.$$

Analogous notation is used for row replacements and interchanges.

Definition 2.25. The *rank* of an $m \times n$ matrix $\mathbf{A}$, denoted by $\operatorname{rank}(\mathbf{A})$, is the maximal number of linearly independent columns (or rows) of $\mathbf{A}$. Equivalently, the *rank* of $\mathbf{A}$ is defined to be the dimension of its column space (or row space).

The following theorem summarizes some important properties of determinants [26, Theorems 2.2, 2.3 & 3.26], [33, p. 462-465].

Theorem 2.26. *Let $\mathbf{A}$ be a square matrix of order n. Then the determinant,* $\det(\mathbf{A})$*, satisfies the following properties.*

1) *The value of the determinant remains unchanged if a scalar multiple of one row (or column) is added to another row (or column).*

2) *The determinant of a triangular matrix is the product of its diagonal entries.*

3) *Taking the transpose of a matrix does not alter its determinant, so* $\det(\mathbf{A}^T) = \det(\mathbf{A})$.

4) $\det(\mathbf{A}) \neq 0$ *if and only if* $\operatorname{rank}(\mathbf{A}) = n$.

For a matrix subdivided into four blocks, the following identities can often help to simplify the calculation of the determinant. The proofs of these results can be found in [33, p. 467 & 475].

Proposition 2.27. *If* $\mathbf{A}$ *and* $\mathbf{D}$ *are square matrices over an arbitrary field, then*

$$\det\left[\begin{array}{c|c} \mathbf{A} & \mathbf{B} \\ \hline \mathbf{0} & \mathbf{D} \end{array}\right] = \det(\mathbf{A})\det(\mathbf{D}) = \det\left[\begin{array}{c|c} \mathbf{A} & \mathbf{0} \\ \hline \mathbf{C} & \mathbf{D} \end{array}\right].$$

Proposition 2.28. *If* $\mathbf{A}$ *and* $\mathbf{D}$ *are square matrices, then*

$$\det\left[\begin{array}{c|c} \mathbf{A} & \mathbf{B} \\ \hline \mathbf{C} & \mathbf{D} \end{array}\right] = \begin{cases} \det(\mathbf{A})\det\left(\mathbf{D} - \mathbf{C}\mathbf{A}^{-1}\mathbf{B}\right) & \textit{if } \mathbf{A}^{-1} \textit{ exists,} \\ \det(\mathbf{D})\det\left(\mathbf{A} - \mathbf{B}\mathbf{D}^{-1}\mathbf{C}\right) & \textit{if } \mathbf{D}^{-1} \textit{ exists.} \end{cases}$$

Chapter 3

Elliptic Curves and Congruent Numbers

3.1 Overview

This chapter provides a brief introduction to elliptic curves and their properties. There are no new results in this chapter; its purpose is simply to present the background theory necessary to appreciate and understand the results discussed in subsequent chapters. We begin by formally defining elliptic curves and their corresponding group law. Several key theorems, including Mordell's theorem, the Nagell-Lutz theorem, and Mazur's theorem, are also discussed. The torsion subgroup is introduced, and then calculated for congruent number elliptic curves. The final two sections in the chapter are devoted to studying the rank of elliptic curves, with an emphasis on techniques for computing this quantity. The chapter concludes with a discussion of an important result by Monsky that allows the 2-Selmer rank of congruent number elliptic curves to be calculated.

3.2 An Introduction to Elliptic Curves

An elliptic curve over a field K is a non-singular, projective, cubic algebraic curve with a specified base point defined over K. In the projective space $\mathbb{P}^2$, an elliptic curve has the general form, known as the *projective long Weierstrass normal form*,

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3, \tag{3.1}$$

where $a_1, a_2, a_3, a_4, a_6 \in K$ [23, 47, 51, 52]. The base point on this curve in homogeneous coordinates is $\mathscr{O} = [0 : 1 : 0]$. It is referred to as the *point at infinity* and is the only point with $Z = 0$ [23, 25, 47, 51, 52]. An introduction to projective algebraic geometry, including the following definition, can be found in Appendix A of [52].

Definition 3.1. The *projective plane*, $\mathbb{P}^2$, is the set of equivalence classes of triples $[a : b : c]$ with a, b, c not all equal to zero satisfying the equivalence relation

$$[a : b : c] \sim [a' : b' : c'] \text{ if } a = ta', b = tb', c = tc' \text{ for some } t \neq 0.$$

An equivalence class of triples $[a, b, c]$ is called a *point in* $\mathbb{P}^2$, and the numbers a, b, c are called *homogeneous coordinates* for the point $[a, b, c]$ in $\mathbb{P}^2$.

By substituting $x = X/Z$ and $y = Y/Z$ into Equation (3.1), the Weierstrass curve can be written in non-homogeneous coordinates as

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6. \tag{3.2}$$

This is referred to as the *long Weierstrass normal form.* Furthermore, if the characteristic of the field K is not equal to two, a change of variables can be made [51] in Equation (3.2):

$$y \mapsto y - \frac{1}{2}(a_1x + a_3).$$

The simplified equation that results from this substitution is

$$E : y^2 = x^3 + ax^2 + bx + c, \tag{3.3}$$

where

$$a = \frac{1}{4}a_1^2 + a_2, \qquad b = \frac{1}{2}a_1a_3 + a_4, \qquad \text{and} \qquad c = \frac{1}{4}a_3^2 + a_6.$$

This is known as the *reduced Weierstrass equation.*

Recall that for such a curve to be considered an elliptic curve, it must be *non-singular.* That is, it has distinct roots or equivalently its discriminant, given by

$$D = -4a^3c + a^2b^2 + 18abc - 4b^3 - 27c^2, \tag{3.4}$$

is not equal to zero [52]. This implies that elliptic curves over $K \subset \mathbb{R}$ must either have three real roots (as shown in Figure 3.1), or a single real root and a pair of complex conjugate roots (as shown in Figure 3.2). Cubic curves with repeated roots are not elliptic curves; examples of singular cubic curves are shown in Figures 3.3 and 3.4.

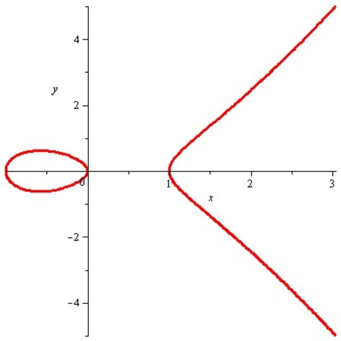


Figure 3.1: The elliptic curve $y^2 = x(x-1)(x+1)$ has three real roots.

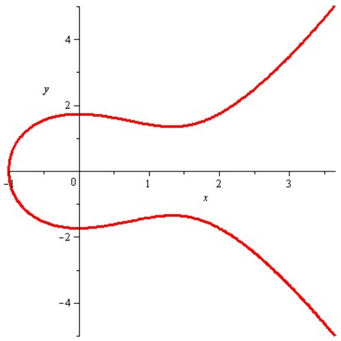


Figure 3.2: The elliptic curve $y^2 = (x+1)(x^2 - 3x + 3)$ with a single real root.

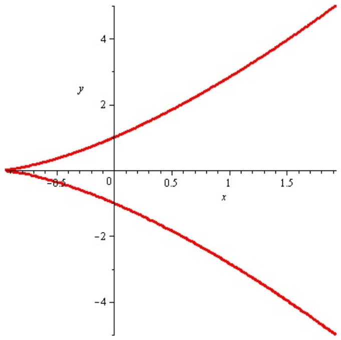


Figure 3.3: The singular cubic curve $y^2 = (x+1)^3$ with a triple root at $x = -1$.

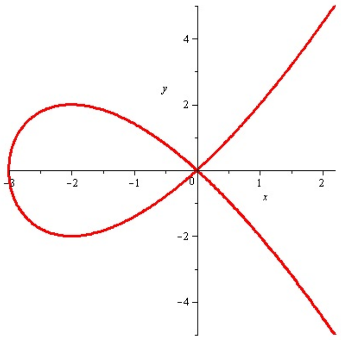


Figure 3.4: The singular cubic curve $y^2 = x^2(x+1)$ has a double root at $x = 0$.

3.3 The Group Law on Elliptic Curves and Mordell's Theorem

A fundamental property of elliptic curves is that their points form an abelian group under a specific binary operation. To investigate this property, we begin by considering the binary algebraic structure that consists of the set of rational points on the elliptic curve E over the field K, along with the binary operation $*$. The line connecting two rational points P and Q on E intersects the curve at a third point, R, defined to be $P * Q$. This process, known as the *chord-tangent composition law* [23], can be applied regardless of whether P and Q are distinct points (Figure 3.5). In the case where $P = Q$, the line drawn is tanget to the curve at that point, so P is a point of multiplicity two. Since P and Q are rational points on the curve E, the line joining them is a rational line, and hence $R = P * Q$ is also a rational point [23, 29, 52]. Thus, given a small number of rational points, the chord-tangent law can be used to generate many other rational points on E.

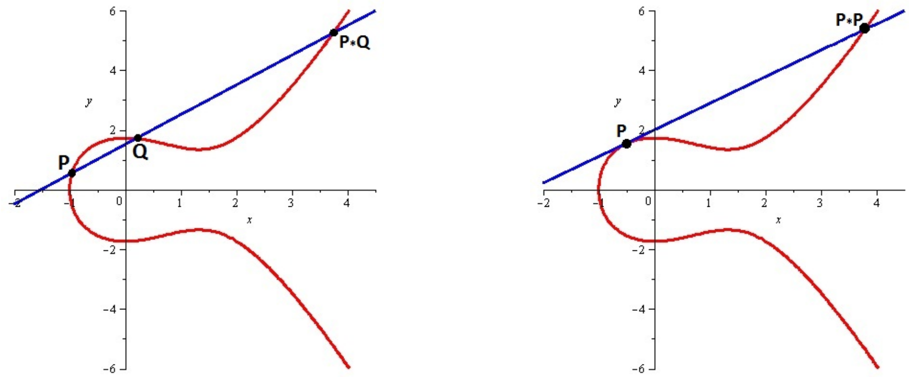


Figure 3.5: The chord-tangent composition law applied to distinct points P and Q, shown on the left, and a single point P, shown on the right, on the elliptic curve $y^2 = (x + 1)(x^2 - 3x - 3)$.

Unfortunately, the chord-tangent composition law lacks an identity element, so it cannot be considered a group law. To resolve this issue, we count the point at infinity, $\mathscr{O}$, as a rational point and define the set of K-rational points on the elliptic curve E to be

$$E(K) = \{(x, y) \in E : x, y \in K\} \cup \{\mathscr{O}\}.$$

By coupling the set $E(K)$ with the chord-tangent law, we can define a new binary operation $+$ that makes $E(K)$ into an abelian group; the point at infinity serves as the identity element for this group. To add two points $P, Q \in E(K)$, we begin by using the chord-tangent law to find the point $P*Q$. If $P*Q \neq \mathscr{O}$ and a line is drawn through the points $P*Q = (x_{pq}, y_{pq})$ and $\mathscr{O}$, the resulting third point of intersection between the curve E and the line is $\mathscr{O} * (P * Q)$; this point is defined to be $P + Q$ [23, 29, 47, 51, 52]. As shown in Figure 3.6, the line through $P * Q$ and $\mathscr{O}$ is a vertical line, so the point $P + Q$ is simply the reflection of the point $P * Q$ about the x-axis. Thus, $P + Q = (x_{pq}, -y_{pq})$. Note that if $P * Q = \mathscr{O}$, then $P + Q$ is defined to be $\mathscr{O}$.

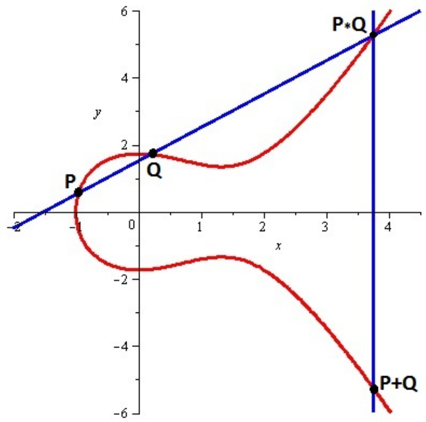


Figure 3.6: The group law operator $+$ applied to the points P and Q on the elliptic curve $y^2 = (x+1)(x^2-3x-3)$.

This important result is summarized by the following theorem [23, 47].

Theorem 3.2. *For the elliptic curve E over the field K, the set $E(K)$ of rational points is an abelian group under the binary operation $+$ defined above. The point at infinity $\mathscr{O}$ is the identity element in the group.*

This means that the following properties hold for the group law operator $+$:

1) **Closure:** If $P, Q \in E(K)$, then $P + Q \in E(K)$.

2) **Associativity:** $(P+Q)+R = P+(Q+R)$ for all $P, Q, R \in E(K)$.

3) **Identity Element:** $P + \mathscr{O} = \mathscr{O} + P = P$ for all $P \in E(K)$.

4) **Inverse:** For every $P \in E(K)$, there exists a point $-P \in E(K)$ such that $P + (-P) = \mathscr{O}$.

5) **Commutativity:** $P + Q = Q + P$ for all $P, Q \in E(K)$.

Each of these properties is simple to verify except for associativity; additional details regarding this can be found in [47, 51, 52].

The precise coordinates of the point $P+Q$ can be determined as follows. Let $P = (x_1, y_1)$ and $Q = (x_2, y_2)$ be points on the elliptic curve E given by Equation (3.3)

$$y^2 = x^3 + a_2x^2 + a_4x + a_6.$$

By the chord-tangent law, we know that the points P and Q are connected by a line of the form $y = \lambda x + \nu$. Substituting this into $x^3 + a_2x^2 + a_4x + a_6 - y^2 = 0$ and simplifying yields

$$x^3 + (a_2 - \lambda^2)x^2 + (a_4 - 2\lambda\nu)x + (a_6 - \nu^2) = 0. \tag{3.5}$$

The third point of intersection between the line $y = \lambda x + \nu$ and the curve E is $P * Q = (x_3, y_3)$, so the cubic polynomial in Equation (3.5) has roots x_1, x_2, and x_3. Therefore, we can write

$$\begin{aligned}&x^3 + (a_2 - \lambda^2)x^2 + (a_4 - 2\lambda\nu)x + (a_6 - \nu^2)\\ &= (x - x_1)(x - x_2)(x - x_3)\\ &= x^3 - (x_1 + x_2 + x_3)x^2 + (x_2x_3 + x_1x_3 + x_1x_2)x - (x_1x_2x_3).\end{aligned}$$

Equating the coefficients of the x^2 terms on each side of the above equation, and solving for x_3 yields

$$x_3 = \lambda^2 - a_2 - x_1 - x_2, \tag{3.6}$$

which is the x-coordinate of the point $P * Q$.

If $P = (x_1, y_1)$ and $Q = (x_2, y_2)$ are points with $x_1 \neq x_2$, then

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1}, \qquad \text{and} \qquad \nu = y_1 - \lambda x_1 = y_2 - \lambda x_2. \tag{3.7}$$

The corresponding y-coordinate for $P * Q = (x_3, y_3)$ can be found by using the equation

$$y_3 = \lambda x_3 + \nu$$

with the values of x_3, λ, and ν given in Equations (3.6) and (3.7). Since $P+Q$ is the reflection of $P * Q$ about the x-axis, it follows that $P + Q = (x_3, -y_3)$.

If $P = Q$, the line $y = \lambda x + \nu$ lies tangent to the curve E at the point P. When $y_1 \neq 0$, the slope of this tangent line is

$$\lambda = \frac{3x_1^2 + 2a_2x_1 + a_4}{2y_1},$$

which is found by implicitly differentiating the elliptic curve equation E with respect to x and then evaluating the resulting equation at $P = (x_1, y_1)$. Substituting this value for λ into Equation (3.6) and simplifying yields

$$x(2P) = \frac{x_1^4 - 2a_4x_1^2 - 8a_6x_1 + a_4^2 - 4a_2a_6}{4y_1^2}. \tag{3.8}$$

This equation is known as the *duplication formula for the x-coordinate of P* and is used to compute the x-coordinate of the point $2P = P + P$. The y-coordinate of $2P$ can be found by following an analogous process to the one outlined above in the case where $P = (x_1, y_1)$ and $Q = (x_2, y_2)$ are points with $x_1 \neq x_2$.

This procedure for determining the precise coordinates of the point $P+Q$ is known as the group law algorithm and is described in detail for general Weierstrass curves in [51].

A well-known theorem proved by Louis Mordell in 1922 provides further insight into the structure of the group of rational points on a rational elliptic curve [23, 25, 29, 51, 52, 59].

Theorem 3.3 (**Mordell's Theorem**). *Let E be an elliptic curve over the field of rational numbers. The group of rational points, $E(\mathbb{Q})$, is a finitely generated abelian group.*

Proof. See Chapter 6 of [23], Chapter VIII.4 of [51], or Chapter III of [52]. □

Because the group of rational points $E(\mathbb{Q})$ forms a finitely generated abelian group, the fundamental theorem of finitely generated abelian groups (Theorem 2.3) can be applied to write $E(\mathbb{Q})$ as a direct sum of cyclic groups

$$E(\mathbb{Q}) \cong \mathbb{Z}_{p_1^{\nu_1}} \oplus \mathbb{Z}_{p_2^{\nu_2}} \oplus \cdots \oplus \mathbb{Z}_{p_\omega^{\nu_\omega}} \oplus \underbrace{\mathbb{Z} \oplus \mathbb{Z} \oplus \cdots \oplus \mathbb{Z}}_{r \text{ copies}},$$

where $\mathbb{Z}$ is an infinite cyclic group and $\mathbb{Z}_{p_i^{\nu_i}}$ is a finite cyclic group with prime-power order for all $i \in [1, \omega]$. This can be stated more concisely as

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

where $\mathscr{T} \cong \mathbb{Z}_{p_1^{\nu_1}} \oplus \mathbb{Z}_{p_2^{\nu_2}} \oplus \cdots \oplus \mathbb{Z}_{p_\omega^{\nu_\omega}}$ denotes the torsion subgroup and $r \in \mathbb{N}$ is called the *arithmetic rank*, or *Mordell-Weil rank*, of the elliptic curve E. The torsion subgroup is relatively easy to compute and will be discussed in detail in Section 3.4. However, the rank is not nearly as well understood, because there does not exist an effective method for calculating it in all cases. The determination of the rank is crucial when it comes to studying congruent and non-congruent numbers; more information regarding this mysterious quantity will be presented in Section 3.5.

3.4 The Torsion Subgroup

We begin by stating the definition of the torsion subgroup [23, 29, 51, 52].

Definition 3.4. The *torsion subgroup*, $\mathscr{T}$, of $E(\mathbb{Q})$ is the group consisting of all rational points of finite order on the elliptic curve E.

Therefore, to find the rational points that belong to the torsion subgroup, we must recall the definition of the order of a point $P \in E(K)$ [52].

Definition 3.5. Let E be an elliptic curve and let $P = (x, y)$ be a point in $E(K)$. The point P has *finite order* if there exists $m \in \mathbb{N}^+$ such that

$$mP = \underbrace{P + P + \cdots + P}_{m \text{ copies}} = \mathscr{O},$$

but $m'P \neq \mathscr{O}$ for all integers $m' \in [1, m)$. The integer m is called the *order of* P. If no such integer m exists, then P has *infinite order.*

Clearly, the point at infinity has order one, and since this is a point of finite order on every elliptic curve, the torsion subgroup is guaranteed to contain at least one element. Points $P = (x, y)$ of order two are also simple to find, as they statisfy $2P = \mathscr{O}$ with $P \neq \mathscr{O}$. An equivalent way of writing $2P = P + P = \mathscr{O}$ is $P = -P$, which means that $(x, y) = (x, -y)$. This only holds if $y = -y$, so $y = 0$. Thus, points of order two have the form $(x, 0)$ [52]. Other rational points of finite order on an elliptic curve can be found by using a well-known theorem proven independently by Nagell and Lutz [51, 52, 59].

Theorem 3.6 (**Nagell-Lutz Theorem**). *Let*

$$y^2 = f(x) = x^3 + ax^2 + bx + c$$

be a non-singular cubic curve with $a, b, c \in \mathbb{Z}$*, and let*

$$D = -4a^3c + a^2b^2 + 18abc - 4b^3 - 27c^3$$

be the discriminant of $f(x)$*. Let* $P = (x, y)$ *be a rational point of finite order. Then* x *and* y *are integers and either* $y = 0$ *or else* y^2 *divides* D*.*

Proof. See Chapter VIII.7 of [51] or Chapter II of [52]. □

It should be emphasized that the Nagell-Lutz theorem is not an if-and-only-if statement. Therefore, points on the curve with integer coordinates satisfying $y^2 \,|D$ are unfortunately not guaranteed to have finite order. However, if $P = (x, y)$ is a rational point of finite order, then $2P$ must also have finite order. By Theorem 3.6, rational points of finite order have integer coordinates. The duplication formula for the x-coordinate of P, stated in Equation (3.8), can be applied to compute the x-coordinate of $2P$. If $x(2P)$ is found not to be an integer, $2P$ is not a point of finite order, and hence P also is not a point of finite order.

An alternate technique for determining the points of finite order on a non-singular cubic curve involves defining a reduction modulo p map that is an isomorphism. This method is summarized by the following theorem [52].

Theorem 3.7 (**Reduction Modulo *p* Theorem**). *Let C be a non-singular cubic curve*

$$y^2 = x^3 + ax^2 + bx + c$$

with $a, b, c \in \mathbb{Z}$, and let D be the discriminant

$$D = -4a^3c + a^2b^2 + 18abc - 4b^3 - 27c^2.$$

Let $\Phi \subseteq C(\mathbb{Q})$ be the subgroup consisting of all points of finite order. For any prime p, let $P \mapsto \widetilde{P}$ be the reduction modulo p map

$$\Phi \longrightarrow \widetilde{C}(\mathbb{F}_p), \qquad P \mapsto \widetilde{P} = \begin{cases} (\widetilde{x}, \widetilde{y}) & \text{if } P = (x, y), \\ \widetilde{\mathscr{O}} & \text{if } P = \mathscr{O}. \end{cases}$$

If p does not divide $2D$, then the reduction modulo p map is an isomorphism of Φ onto a subgroup of $\widetilde{C}(\mathbb{F}_p)$.

Proof. See Section 4.3 of [52]. □

Both the Nagell-Lutz theorem and the reduction modulo p theorem provide methods for finding the points of finite order on an elliptic curve. However, to completely characterize the torsion subgroup of the curve, we utilize a powerful result by Mazur [23, 29–31, 51, 52, 59].

Theorem 3.8 (**Mazur's Theorem**). *For an elliptic curve E defined over $\mathbb{Q}$, the torsion subgroup, $\mathscr{T}$, of the group of rational points, $E(\mathbb{Q})$, is isomorphic to one of the following fifteen groups:*

1) *A cyclic group of order N, $\mathbb{Z}_N$, with $1 \leq N \leq 10$ or $N = 12$.*

2) *The product of a cyclic group of order two and a cyclic group of order $2N$, $\mathbb{Z}_2 \times \mathbb{Z}_{2N}$, with $1 \leq N \leq 4$.*

Proof. See [30] and [31]. □

Of specific interest to this thesis is the torsion subgroup of congruent number elliptic curves $E_n : y^2 = x(x-n)(x+n)$. By inspection, it is clear that these curves have exactly three points of order two, $(0,0)$, $(n,0)$, and $(-n,0)$. Combining these three points with the point at infinity allows us to deduce that congruent number elliptic curves have at least four rational points of finite order. We would like to show that these four points are the only torsion points on E_n. We follow a method similar to that presented in [22, 25].

We begin by proving a lemma that enables us to calculate the number of points on the curve E_n over the finite field $\mathbb{F}_p$ for a prime p with $p \equiv 3 \pmod 4$.

Lemma 3.9. *If p is a prime with $p \nmid n$ and $p \equiv 3 \pmod 4$, then the curve E_n over $\mathbb{F}_p$ has exactly $p+1$ points.*

Proof. The points $\mathscr{O}$, $(0,0)$, and $(\pm n, 0)$ always lie on the curve E_n. We will verify that these four points are distinct over $\mathbb{F}_p$. In homogeneous coordinates, the points $\mathscr{O}$, $(0,0)$, and $(\pm n,0)$ are written as $[0:1:0]$, $[0:0:1]$, and $[\pm n : 0 : 1]$, respectively. According to Definition 3.1, two sets of coordinates represent the same point in projective space if and only if the coordinates differ by a nonzero constant. This means that the point at infinity cannot equal $(0,0)$ or $(\pm n,0)$ over $\mathbb{F}_p$. Furthermore, equality of any two of $(0,0)$ or $(\pm n,0)$ leads to the congruences

$$\pm n \equiv 0 \pmod p \qquad \text{or} \qquad n \equiv -n \pmod p.$$

By assumption $p \equiv 3 \pmod 4$, so p is odd. Therefore, in order for the above congruences to hold, we require that $p|n$, which contradicts our initial assumption that $p \nmid n$. Thus, $\mathscr{O}$, $(0,0)$, and $(\pm n,0)$ are distinct points over $\mathbb{F}_p$.

We treat the cases $p = 3$ and $p > 3$ separately. When $p = 3$,

$$y^2 = x^3 - n^2 x = x(x^2 - n^2) \equiv \begin{cases} 0 \pmod p & \text{if } p|x, \\ x(1-n^2) \pmod p & \text{if } p \nmid x. \end{cases}$$

By assumption $p \nmid n$, so Fermat's little theorem (Theorem 2.14) implies that

$$(1 - n^2) \equiv 0 \pmod p$$

for $p = 3$. Therefore, irrespective of whether p divides x, we have

$$y^2 = x(x-n)(x+n) \equiv 0 \pmod p.$$

This shows that $\mathscr{O}$, $(0,0)$, and $(\pm n, 0)$ are the only possible points on E_n when $p=3$, so there are exactly $p+1=4$ points on E_n over $\mathbb{F}_3$.

Let us now consider the case where $p>3$ and examine the points for which $x \neq 0, \pm n$. Since we are working modulo p, there are $(p-3)$ such values for x. By assumption p is odd, so $(p-3)$ is even. As a result, we can group the $(p-3)$ values for x into pairs $\{\pm x\}$. Clearly there is a point on E_n whenever (x^3-n^2x) is a square in $\mathbb{F}_p$. Therefore, we treat two cases, one where (x^3-n^2x) is a square and one where it is not a square. We begin by assuming that (x^3-n^2x) is a square in $\mathbb{F}_p$, and apply Theorem 2.17 to deduce that

$$\left(\frac{(x^3-n^2x)}{p}\right)=1. \tag{3.9}$$

Since $p \equiv 3 \pmod 4$, it follows from Theorem 2.17, Theorem 2.19, and Equation (3.9) that

$$\left(\frac{((-x)^3-n^2(-x))}{p}\right)=\left(\frac{-1}{p}\right)\left(\frac{(x^3-n^2x)}{p}\right)=-1.$$

This enables us to conclude that $((-x)^3-n^2(-x))$ is a quadratic nonresidue of p, and hence it is not a square in $\mathbb{F}_p$.

An analogous argument can be used to show that when (x^3-n^2x) is not a square in $\mathbb{F}_p$, then $((-x)^3-n^2(-x))$ is a square. Thus, every pair $\{\pm x\}$ leads to exactly one point on E_n over $\mathbb{F}_p$. This means that only half of the $(p-3)$ distinct x values contained by the pairs $\{\pm x\}$ need to be considered. Each of these $(p-3)/2$ values for x corresponds to two y values, $\pm y$. Neglecting the points $\mathscr{O}$, $(0,0)$, and $(\pm n,0)$, there are $(p-3)$ points on E_n over $\mathbb{F}_p$. Thus, altogether there are $(p+1)$ points on E_n over $\mathbb{F}_p$. □

The following theorem completely characterizes the torsion subgroup of congruent number elliptic curves.

Theorem 3.10. *For the congruent number elliptic curve E_n, $|\mathscr{T}_n|=4$ and $\mathscr{T}_n \cong \mathbb{Z}_2 \times \mathbb{Z}_2$.*

Proof. We know that the four torsion points $\mathscr{O}$, $(0,0)$, and $(\pm n,0)$ lie on the curve E_n. By way of contradiction, assume there is another torsion point on E_n. This torsion point cannot be a point of order two, so it must have order greater than two. Since $\mathscr{T}_n$ contains three points of order two and at least one with order greater than two, Mazur's Theorem (Theorem 3.8) implies that $\mathscr{T}_n$ is isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_{2N}$ with $N \in \{2,3,4\}$. Notice that $\mathbb{Z}_2 \times \mathbb{Z}_4$ is a group of order eight, so Theorem 2.4 can be applied to deduce that it has subgroups of order 1, 2, 4, and 8. Similarly, Theorem 2.4 implies that $\mathbb{Z}_2 \times \mathbb{Z}_6$ has subgroups of order 1, 2, 3, 4, 6, and 12, and $\mathbb{Z}_2 \times \mathbb{Z}_8$ has subgroups of order 1, 2, 4, 8, and 16. Therefore, regardless of which of the three groups the torsion subgroup $\mathscr{T}_n$ is isomorphic to, $\mathscr{T}_n$ contains a subgroup $H = \{P_1, P_2, \ldots, P_m\}$ of order m, where m is equal to either three or eight.

Consider the reduction modulo p map $P \mapsto \widetilde{P}$. By Theorem 3.7, we know that if p does not divide $2D$, where D is the discriminant of E_n, then the reduction modulo p map is an isomorphism of $\mathscr{T}_n$ onto a subgroup of $\widetilde{E_n}(\mathbb{F}_p)$. It follows that the reduction map $P \mapsto \widetilde{P}$ is injective on H for all primes $p > 2D$. Thus, m divides the order of the group $\widetilde{E_n}(\mathbb{F}_p)$ for all such p. Notice that for the curve E_n, the discriminant, given by Equation (3.4), reduces to $D = 4n^6$. Since $p > 2D = 8n^6$, clearly $p \nmid n$. Therefore, if $p \equiv 3 \pmod 4$, we can apply Lemma 3.9 to deduce that $|\widetilde{E_n}(\mathbb{F}_p)| = p + 1$. For primes p with $p > 2D$, we know that m divides the order of $\widetilde{E_n}(\mathbb{F}_p)$, so $m|(p+1)$, or equivalently $p \equiv -1 \pmod m$. This implies that for all but a finite number of primes p with $p \equiv 3 \pmod 4$, we have

$$p \equiv -1 \pmod m.$$

By Dirichlet's Theorem on Primes in Arithmetic Progressions (Theorem 2.20), we know that for positive integers a and b with $(a, b) = 1$, there are infinitely many primes p with $p \equiv b \pmod a$.

When $m = 8$, all but a finite number of primes p with $p \equiv 3 \pmod 4$ satisfy the congruence $p \equiv -1 \pmod 8 \equiv 7 \pmod 8$. This means that if $m = 8$, there are only finitely many primes with $p \equiv 3 \pmod 8$, which contradicts Dirichlet's Theorem (Theorem 2.20).

Now suppose $m = 3$. Then for all but finitely many primes p with $p \equiv 3 \pmod 4$, we have $p \equiv -1 \pmod 3$. Solving this system of congruences by using the Chinese Remainder Theorem (Theorem 2.13) yields $p \equiv 11 \pmod{12}$. Therefore, when $m = 3$, there can only be finitely many primes $p \equiv 7 \pmod{12}$, which contradicts Dirichlet's Theorem (Theorem 2.20).

Thus, the only rational points of finite order on the congruent number elliptic curve E_n are $\mathscr{O}$, $(0,0)$, and $(\pm n, 0)$, so $|\mathscr{T}_n| = 4$ and by Mazur's Theorem (Theorem 3.8), $\mathscr{T}_n \cong \mathbb{Z}_2 \times \mathbb{Z}_2$. □

3.5 The Arithmetic Rank and the Method of Complete 2-Descent

In Section 3.3, the concept of rank was introduced when we applied Mordell's Theorem in conjunction with the fundamental theorem of finitely generated abelian groups to write

$$E(\mathbb{Q}) \cong \mathscr{T} \oplus \mathbb{Z}^r.$$

The arithmetic rank can formally be defined as follows.

Definition 3.11. Let E be an elliptic curve and let $E(\mathbb{Q})$ be its group of rational points. The *arithmetic rank* of E, denoted by r, is the number of generators with infinite order $\mathbb{Z}$ in $E(\mathbb{Q})$. Equivalently, the *arithmetic rank* is the number of independent rational points of infinite order on E. The *arithmetic rank* is also known as the *Mordell-Weil rank*.

Calculating the arithmetic rank of elliptic curves is, in most cases, a difficult and computationally challenging problem. Currently, there do not exist methods for computing the rank of all elliptic curves. It has been conjectured that the rank can be arbitrarily large [51], but finding elliptic curves with even moderately high rank is a difficult task. Bhargava and Shankar proved that the average rank of all elliptic curves over $\mathbb{Q}$ is at most 1.17 and that a positive proportion of the curves have rank zero [3]. Therefore, because moderate and high-rank elliptic curves are scarce, finding curves with rank greater than one is a problem of interest.

In 2006, Elkies discovered an elliptic curve with rank equal to at least 28; the precise value of the rank is still unknown. The elliptic curve with the largest known rank is

$$\begin{gathered} y^2 + xy + y = x^3 - x^2 + 31368015812338065133318565292206590792820353345x \\ +302038802698566087335643188429543498624522041683874493555186062568159847. \end{gathered}$$

This curve was found by Elkies in 2009, and its rank is equal to 19. Rogers currently holds the record for the largest-rank congruent number elliptic curve with $r(n) = 7$ for $n = 797507543735$ [45]. Additional information regarding high-rank elliptic curves can be found in [9, 10].

Recall from Lemma 1.2 that the arithmetic rank $r(n)$ of congruent number elliptic curves, which have the form $y^2 = x^3 - n^2x$, is related to the congruent number problem; if $r(n) > 0$, then n is a congruent number. Alter, Curtz, and Kubota [1] conjectured that integers of the form $n \equiv 5, 6, 7$

(mod 8) are congruent. By using both the Birch and Swinnterton-Dyer conjecture and the Shafarevich-Tate conjecture, Lagrange [10, 27, 49] was able to expand upon Alter, Curtz, and Kubota's work and state the following conjecture for the parity of $r(n)$:

$$r(n) \equiv \begin{cases} 0 \pmod 2 & \text{if } n \equiv 1, 2, 3 \pmod 8, \\ 1 \pmod 2 & \text{if } n \equiv 5, 6, 7 \pmod 8. \end{cases}$$

This would imply that integers n satisfying $n \equiv 5, 6, 7 \pmod 8$ are congruent numbers.

Monsky provided evidence supporting the above conjecture when he used the link between congruent numbers and elliptic curves to prove that certain numbers n with at most two distinct odd prime divisors are congruent [34]. Monsky's families of congruent numbers $n \equiv 5, 6, 7 \pmod 8$ have the form

1) p_5, p_7, $2p_7$, and $2p_3$,

2) p_3p_7, p_3p_5, $2p_3p_5$, and $2p_5p_7$,

3) p_1p_5 with $\left(\dfrac{p_1}{p_5}\right) = -1$,

4) p_1p_7 and $2p_1p_7$ with $\left(\dfrac{p_1}{p_7}\right) = -1$,

5) $2p_1p_3$ with $\left(\dfrac{p_1}{p_3}\right) = -1$,

where p_i denotes primes that are congruent to $i \pmod 8$.

Tian expanded upon Monsky's results and described the first families of congruent numbers with arbitrarily many prime divisors [7, 54, 55]. His congruent numbers have one prime factor congruent to 3, 5, or 7 modulo 8 and arbitrarily many prime factors congruent to 1 modulo 8. Tian also proved the following important theorem [7, 54, 55].

Theorem 3.12. *For any given integer $k \geq 0$, there are infinitely many square-free congruent numbers with exactly $k+1$ odd prime divisors in each residue class of 5, 6, and 7 modulo 8.*

Methods known as descents are often applied to determine the rank of an elliptic curve. These techniques have an extensive history dating back to the method of infinite decent. Fermat developed this technique and used it to prove that no right triangle with integer side lengths can have its area equal to an integer squared [5]. A complete 2-descent is a method that we can apply to calculate an upper bound for the rank of an elliptic curve. This algorithm attempts to find the generators for the quotient group $E_n(\mathbb{Q})/2E_n(\mathbb{Q})$ by determining whether specific pairs of equations are solvable. The complete 2-descent algorithm for elliptic curves with a Weierstrass equation of the form $y^2 = (x - e_1)(x - e_2)(x - e_3)$ over a field K is stated and proved in Section X.1 of [51]. The version of this theorem for congruent number elliptic curves is stated in [10, Theorem 1] and [49, Theorem 3.1] and is described by the following theorem.

Theorem 3.13 (Complete 2-Descent for $\boldsymbol{E_n}$). *Let $p_1, p_2, \ldots, p_t$ for $t \in \mathbb{N}^+$ be distinct odd primes and*

$$n = 2^{\epsilon} p_1 p_2 \cdots p_t$$

be a positive integer with $\epsilon \in \{0, 1\}$. Let E_n be the elliptic curve over $\mathbb{Q}$ defined by the equation

$$E_n : y^2 = x^3 - n^2 x = x(x - n)(x + n),$$

and

$$\mathbb{Q}(S, 2) := \{c \in \mathbb{Q}^*/\mathbb{Q}^{*2} |\ v_p(c) \equiv 0 \pmod{2}\ \ \forall\, p \in M_{\mathbb{Q}} \backslash S\},$$

where $v_p(c)$ is the p-adic valuation of c and $S = \{\infty, 2, p_1, \ldots, p_t\}$ is a finite subset of $M_{\mathbb{Q}}$, the set of all places of $\mathbb{Q}$. Then there is an injective homomorphism

$$b\colon E_n(\mathbb{Q})/2E_n(\mathbb{Q}) \longrightarrow \mathbb{Q}(S, 2) \times \mathbb{Q}(S, 2) \tag{3.10}$$

defined for $P = (x, y)$ by

$$b(P) = \begin{cases} (1, 1) & \textit{if} \quad P = \mathscr{O}, \\ (-1, -n) & \textit{if} \quad P = (0, 0), \\ (n, 2) & \textit{if} \quad P = (n, 0), \\ (x, x - n) & \textit{if} \quad P = (x, y) \neq \mathscr{O}, (0, 0), (n, 0). \end{cases}$$

If $(b_1, b_2) \in \mathbb{Q}(S, 2) \times \mathbb{Q}(S, 2) \backslash \{(1, 1), (-1, -n), (n, 2)\}$, then $(b_1, b_2) \in \operatorname{Im}(b)$ if and only if the system of equations

$$\left\{\begin{aligned} b_1 z_1^2 - b_2 z_2^2 &= n, \\ b_1 z_1^2 - b_1 b_2 z_3^2 &= -n \end{aligned}\right\} \tag{3.11}$$

has a solution $(z_1, z_2, z_3) \in \mathbb{Q}^* \times \mathbb{Q}^* \times \mathbb{Q}$. In this case,

$$(b_1, b_2) = b(P)$$

for

$$P = (b_1z_1^2, b_1b_2z_1z_2z_3) = (b_2z_2^2 + n, b_1b_2z_1z_2z_3).$$

Recall from Theorem 3.10 that the torsion subgroup of E_n is isomorphic to $\mathbb{Z}_2 \oplus \mathbb{Z}_2$, and hence

$$E_n(\mathbb{Q}) \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}^{r(n)},$$

where $r(n)$ is the arithmetic rank of E_n. Furthermore,

$$E_n(\mathbb{Q})/2E_n(\mathbb{Q}) \cong (\mathbb{Z}_2)^{r(n)+2},$$

and because the homomorphism b defined in Theorem 3.13 is injective,

$$\mathrm{Im}(b) \cong (\mathbb{Z}_2)^{r(n)+2}.$$

This means that there are $2^{r(n)+2}$ pairs (b_1, b_2) for which the system of equations in (3.11) has a solution. Clearly the four torsion points $\mathscr{O}$, $(0,0)$, $(n,0)$, and $(-n,0)$ always lie on E_n. However, since there is no known method for determining whether equations of the form in (3.11) are solvable, it often can be difficult to conclusively ascertain which of the remaining pairs (b_1, b_2) are in $\mathrm{Im}(b)$.

By defining an upper bound B for the number of pairs (b_1, b_2) corresponding to non-torsion points for which the system in (3.11) may be solvable, the following inequality can be established.

$$2^{r(n)+2} \leq B + 4 \qquad \iff \qquad r(n) \leq \log_2\left(\frac{B+4}{4}\right). \tag{3.12}$$

If the precise number of elements in $\mathrm{Im}(b)$ can be determined, then the inequality in (3.12) becomes an equality. In addition, if the only pairs (b_1, b_2) for which the system in (3.11) is solvable correspond to torsion points on E_n, then B is zero and consequently the rank of E_n is also zero. By Lemma 1.2, we know that such rank-zero elliptic curves E_n correspond to non-congruent numbers n.

An example that illustrates how the method of complete 2-descent can be used to conclusively determine the rank of E_n and generate a family of non-congruent numbers can be found in [24]. In this paper, Iskra proves that there exists an infinite set of primes of the form $8k + 3$ satisfying a specific pattern of Legendre symbols, such that any product of primes in this set is a non-congruent number; a detailed proof of the result using the method of complete 2-descent can also be found in Section 4.1 of [38].

3.6 The 2-Selmer Rank of E_n and Monsky's Formula

We now consider the space formed by the intersection of the two conics defined in Equation (3.11). For a given pair (b_1, b_2), these two equations define a new curve

$$C(b_1, b_2) := \begin{cases} \quad b_1 z_1^2 - b_2 z_2^2 = n, \\ b_1 z_1^2 - b_1 b_2 z_3^2 = -n. \end{cases}$$

This is called a *homogeneous space* for the elliptic curve E_n over the field $\mathbb{Q}$, denoted by $E_n/\mathbb{Q}$; more information regarding homogeneous spaces can be found in Chapter X.3 of [51].

Recall from Theorem 3.13 that if there exists a solution $(z_1, z_2, z_3) \in \mathbb{Q}^* \times \mathbb{Q}^* \times \mathbb{Q}$ satisfying $C(b_1, b_2)$ for a given pair (b_1, b_2), then there is a corresponding point in $E_n(\mathbb{Q})/2E_n(\mathbb{Q})$. But determining whether or not a given homogeneous space $C(b_1, b_2)$ has a solution is a challenging task. It is sometimes possible to find rational points on homogeneous spaces by inspection or by conducting searches using computers. Furthermore, for certain values of (b_1, b_2), curves can be eliminated from consideration because they do not have any points over $\mathbb{R}$ or over $\mathbb{Q}_p$ for some prime p; a collection of useful unsolvability conditions is stated in [49]. However, some homogeneous spaces have local solutions for every prime p, but yet do not have a global solution. In this situation, the Hasse principle (Principle 2.24) fails, which makes it difficult to fully determine the elements in $E_n(\mathbb{Q})/2E_n(\mathbb{Q})$.

We define two important sets of homogeneous spaces called the 2-Selmer group and the Shafarevich-Tate group. The *2-Selmer group*, $\mathrm{Sel}_2(E_n/\mathbb{Q})$, is the set consisting of the homogeneous spaces $C(b_1, b_2)$ that have solutions everywhere locally [29]. Because $\mathbb{Q} \subseteq \mathbb{Q}_p$ for all primes $p \geq 2$, the homogeneous spaces in $\mathrm{Im}(b)$, where b is the injective homomorphism described in Equation (3.10), belong to the 2-Selmer group. Therefore, the set of homogeneous spaces in $\mathrm{Sel}_2(E_n/\mathbb{Q})$ with solutions over $\mathbb{Q}$ forms a subgroup that is isomorphic to $E_n(\mathbb{Q})/2E_n(\mathbb{Q})$. The *Shafarevich-Tate group*, $\text{Ш}(E_n/\mathbb{Q})[2]$, is the quotient group of $\mathrm{Sel}_2(E_n/\mathbb{Q})$ by $E_n(\mathbb{Q})/2E_n(\mathbb{Q})$. Thus, the Shafarevich-Tate group is comprised of elements that are equal to $C(1, 1)$ or homogeneous spaces in $\mathrm{Sel}_2(E_n/\mathbb{Q})$ that do not have solutions over the rational numbers [29]. If the Shafarevich-Tate group is trivial, then every homogeneous space that is locally solvable is also globally solvable, and hence corresponds to a rational point on E_n.

The relationship between the groups $E_n(\mathbb{Q})/2E_n(\mathbb{Q})$, $\mathrm{Sel}_2(E_n/\mathbb{Q})$, and

$Ш(E_n/\mathbb{Q})[2]$ is represented by the short exact sequence

$$0 \longrightarrow E_n(\mathbb{Q})/2E_n(\mathbb{Q}) \xrightarrow{\psi} \mathrm{Sel}_2(E_n/\mathbb{Q}) \xrightarrow{\phi} Ш(E_n/\mathbb{Q})[2] \longrightarrow 0,$$

where ψ is a monomorphism, ϕ is an epimorphism, and $\ker(\phi) = \mathrm{Im}(\psi)$ [23, 29, 51]. A thorough discussion of the theory governing the Selmer and Shafarevich-Tate groups can be found in Chapter X.4 of [51].

For the congruent number elliptic curve E_n,

$$|\mathrm{Sel}_2(E_n/\mathbb{Q})| = 2^{2+s(n)},$$

where $s(n)$ is defined to be the *2-Selmer rank* of E_n [10, 19, 20]. The following theorem describes the parity of the 2-Selmer rank of congruent number elliptic curves E_n [20, appendix].

Theorem 3.14. *If n is a positive square-free integer, then*

$$s(n) \equiv \begin{cases} 0 \pmod 2 & \text{if } n \equiv 1, 2, 3 \pmod 8, \\ 1 \pmod 2 & \text{if } n \equiv 5, 6, 7 \pmod 8. \end{cases}$$

Proof. See the appendix by Monsky in [20]. □

The Selmer conjecture claims that $s(n)$ and $r(n)$ have the same parity [19]. In addition, the arithmetic rank and 2-Selmer rank of the elliptic curve E_n are related by the well-known inequality

$$r(n) \leq s(n). \tag{3.13}$$

Notice that if the 2-Selmer rank of E_n is equal to zero, then the above inequality guarantees that the Mordell-Weil rank of the curve is also zero. Thus, n is a non-congruent number.

Monsky, in the appendix of Heath-Brown's paper [20], offered a new perspective on the 2-descent algorithm when he transformed it into a computation involving linear algebra. In his proof of Theorem 3.14, Monsky begins with a pair of equations derived by Heath-Brown in [19], and develops an elegant formula for computing $s(n)$. Monsky's formula calculates the 2-Selmer rank of E_n by relating it to the rank of a matrix with entries defined over $\mathbb{F}_2$. We will refer to this matrix as the Monsky matrix. Monsky's formula for computing the 2-Selmer rank of E_n is essential to the proofs of our main results in Chapters 4, 5, and 6 and is summarized by the following theorem.

Theorem 3.15 (**Monsky's Formula for the 2-Selmer Rank of $\boldsymbol{E_n}$**). *Let n be a square-free positive integer with odd prime factors $p_1, p_2, \ldots, p_m$. The diagonal $m \times m$ matrices $\mathbf{D}_k = [d_i]$ for $k \in \{-2, -1, 2\}$, and the $m \times m$ matrix $\mathbf{A} = [a_{ij}]$ are defined by*

$$d_i = \begin{cases} 0, & \textit{if } \left(\dfrac{k}{p_i}\right) = 1, \\ 1, & \textit{if } \left(\dfrac{k}{p_i}\right) = -1, \end{cases}$$

and

$$a_{ij} = \begin{cases} 0, & \textit{if } \left(\dfrac{p_j}{p_i}\right) = 1,\ j \neq i, \\ 1, & \textit{if } \left(\dfrac{p_j}{p_i}\right) = -1,\ j \neq i, \end{cases} \qquad a_{ii} = \sum_{j:j\neq i} a_{ij}. \tag{3.14}$$

Then the 2-Selmer rank of E_n is

$$s(n) = \begin{cases} 2m - \operatorname{rank}_{\mathbb{F}_2}(\mathbf{M_o}), & \textit{if } n = p_1 p_2 \cdots p_m, \\ 2m - \operatorname{rank}_{\mathbb{F}_2}(\mathbf{M_e}), & \textit{if } n = 2p_1 p_2 \cdots p_m, \end{cases} \tag{3.15}$$

where $\mathbf{M_o}$ and $\mathbf{M_e}$ are the $2m \times 2m$ matrices given by

$$\mathbf{M_o} = \left[\begin{array}{c|c} \mathbf{A} + \mathbf{D_2} & \mathbf{D_2} \\ \hline \mathbf{D_2} & \mathbf{A} + \mathbf{D_{-2}} \end{array}\right], \tag{3.16}$$

and

$$\mathbf{M_e} = \left[\begin{array}{c|c} \mathbf{D_2} & \mathbf{A} + \mathbf{D_2} \\ \hline \mathbf{A}^T + \mathbf{D_2} & \mathbf{D_{-1}} \end{array}\right]. \tag{3.17}$$

Proof. See the appendix in [20]. □

According to Monsky's formula, given by Equation (3.15), for an odd (or even) integer n, E_n has $s(n) = 0$ if and only if the matrix $\mathbf{M_o}$ in Equation (3.16) (or $\mathbf{M_e}$ in Equation (3.17)) has full rank, or equivalently nonzero determinant. Therefore, the inequality in Equation (3.13) that relates the arithmetic rank to the 2-Selmer rank of E_n implies n is a non-congruent number if

$$\det(\mathbf{M_o}) \neq 0 \text{ when } n \text{ is odd,}$$

or

$$\det(\mathbf{M_e}) \neq 0 \text{ when } n \text{ is even.}$$

This idea will form the basis of our method for generating families of non-congruent numbers presented in Chapters 4, 5, and 6.

Chapter 4

Families of Non-congruent Numbers

4.1 Overview

In this chapter, our focus is on generating a new family of even non-congruent numbers with arbitrarily many distinct prime divisors. The first reference to families of non-congruent numbers dates back to a paper by Genocchi published in 1855 [15]. These original families of non-congruent numbers contain a maximum of two distinct odd prime factors. In 1915 Bastien [2] presented two additional families of non-congruent numbers comprised of one or two prime factors. Over a century after the appearance of Genocchi's results, new families of non-congruent numbers having five or fewer prime divisors were described by Lagrange [27] and Serf [49]. These new families were more complex in that they required conditions to be imposed on the prime factors of the numbers and the associated values of the Legendre symbols relating the primes. Since then, families of non-congruent numbers that are a product of arbitrarily many distinct prime factors have been described by Cheng and Guo [6], Feng [11], Feng and Xiong [12], Feng and Xue [13], Goto [16], Iskra [24], Li and Tian [28], Ouyang and Zhang [36, 37], Reinholz et al. [39, 40], and Wang [58].

The purpose of this chapter is to describe a new family of even non-congruent numbers whose factorization contains arbitrarily many distinct primes. The numbers that we generate have prime divisors in each odd congruence class modulo eight. This characteristic distinguishes our family of non-congruent numbers from other known families of even non-congruent numbers that have prime factors belonging to a maximum of three odd congruence classes modulo eight.

This chapter is based on a result that appears in [42].

4.2 A Family of Even Non-congruent Numbers With Arbitrarily Many Prime Factors

Our main theorem describes a new family of even non-congruent numbers containing prime factors in each odd congruence class modulo eight.

Theorem 4.1. *Let $p, q, r, s_1, s_2, \ldots, s_t$ be distinct prime numbers satisfying the following congruence conditions:*

$$\begin{aligned} p &\equiv 1 \pmod{8}, \\ q &\equiv 5 \pmod{8}, \\ r &\equiv 3 \pmod{8}, \\ s_\gamma &\equiv 7 \pmod{8} \ \forall\ 1 \leq \gamma \leq t, \end{aligned}$$

where t is an odd positive integer. In addition, assume that the prime factors satisfy the following Legendre symbol conditions:

$$\left(\frac{q}{p}\right) = \left(\frac{r}{p}\right) = \left(\frac{r}{q}\right) = -1,$$

$$\left(\frac{s_i}{p}\right) = 1 \textit{ for all } i \in [1, t] \textit{ with } i \equiv 0 \pmod{2},$$

and

$$\left(\frac{s_j}{p}\right) = \left(\frac{s_k}{q}\right) = \left(\frac{s_k}{r}\right) = \left(\frac{s_k}{s_l}\right) = -1$$

for all $j \in [1, t]$ with $j \equiv 1 \pmod{2}$ and $1 \leq l < k \leq t$. Then by setting $w = s_1 s_2 \cdots s_t$, we have $n = 2pqrw$ is a non-congruent number with $s(n) = 0$.

Our method of proof for this theorem requires showing that the determinant of the Monsky matrix $\mathbf{M_e}$, stated in Equation (3.17), is nonzero.

Proof. We begin by considering the case where $t = 1$, so $n = pqrs_1$. The Monsky matrix $\mathbf{M_e}$ for n has the form

$$\mathbf{M_e} = \left[\begin{array}{cccc|cccc} 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\ \hline 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 \end{array}\right].$$

A software program, such as Maple, can be used to verify that this matrix has full rank, and hence by Equation (3.15), $s(n) = 0$ and n is a non-congruent number.

We now let t be an odd integer with $t \geq 3$ and construct the $(2t+6) \times (2t+6)$ Monsky matrix $\mathbf{M_e}$ for $n = 2pqrw$. Since some of the entries in $\mathbf{M_e}$ vary depending on the number of prime factors in w, we need to consider two cases, $t \equiv 1 \pmod 4$ or $t \equiv 3 \pmod 4$. These cases are handled simultaneously and the ensuing differences are carefully noted throughout the proof. All of our calculations are carried out over $\mathbb{F}_2$.

The square Monsky matrix of order $(2t+6)$ corresponding to n is given by Equation (3.17),

$$\mathbf{M_e} = \left[\begin{array}{c|c} \mathbf{D_2} & \mathbf{A} + \mathbf{D_2} \\ \hline \mathbf{A}^T + \mathbf{D_2} & \mathbf{D_{-1}} \end{array}\right],$$

where

$$\mathbf{D_2} = \left[\begin{array}{ccc|c} 0 & 0 & 0 & \\ 0 & 1 & 0 & \mathbf{0} \\ 0 & 0 & 1 & \\ \hline & \mathbf{0} & & \mathbf{0_t} \end{array}\right], \qquad \mathbf{D_{-1}} = \left[\begin{array}{ccc|c} 0 & 0 & 0 & \\ 0 & 0 & 0 & \mathbf{0} \\ 0 & 0 & 1 & \\ \hline & \mathbf{0} & & \mathbf{I_t} \end{array}\right],$$

and

$$\mathbf{A} = \left[\begin{array}{ccccccccccc} \beta & 1 & 1 & 1 & 0 & 1 & 0 & 1 & \cdots & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & \cdots & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & \cdots & 1 & 1 \\ 1 & 1 & 0 & 0 & 1 & 1 & 1 & 1 & \cdots & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & \cdots & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & \cdots & 1 & 1 \\ \vdots & \vdots & \vdots & \vdots & & \ddots & \ddots & \ddots & & & \vdots \\ \vdots & \vdots & \vdots & \vdots & & & \ddots & \ddots & \ddots & & \vdots \\ \vdots & \vdots & \vdots & \vdots & & & & \ddots & \ddots & \ddots & \vdots \\ 0 & 1 & 0 & 0 & \cdots & \cdots & \cdots & \cdots & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 & \cdots & \cdots & \cdots & \cdots & 0 & 0 & 0 \end{array}\right],$$

with

$$\beta = \begin{cases} 1 & \text{if } t \equiv 1 \pmod 4, \\ 0 & \text{if } t \equiv 3 \pmod 4. \end{cases}$$

Notice that the final t entries in the first row and the first column of $\mathbf{A}$ exhibit an alternating pattern of ones and zeros.

We perform numerous row and column operations to reduce $\mathbf{M_e}$, so that the value of its determinant can be easily computed. Note that because we are working over $\mathbb{F}_2$, these elementary row and column operations do not alter the determinant of $\mathbf{M_e}$. We list the column and row operations to be applied to $\mathbf{M_e}$ by using the notation introduced at the beginning of Section 2.3.

$$\begin{array}{rcl} C_{t+5} & \longrightarrow & C_{t+4} + C_{t+5} \\ C_{2t+6} & \longrightarrow & C_{2t+6} + C_{t+5} \end{array}$$

$$\text{Even rows} \quad \left\{ \begin{array}{rcl} R_{t+1} & \longrightarrow & R_{t+1} + R_{t+3} \\ R_{t-1} & \longrightarrow & R_{t-1} + R_{t+3} \\ & \vdots & \\ R_6 & \longrightarrow & R_6 + R_{t+3} \\ R_4 & \longrightarrow & R_4 + R_{t+3} \end{array} \right.$$

$$\begin{array}{rcl} R_3 & \longrightarrow & R_3 + R_{t+3} \\ R_2 & \longrightarrow & R_2 + R_{t+3} \end{array}$$

$$\text{Odd rows} \quad \left\{ \begin{array}{rcl} R_t & \longrightarrow & R_t + R_{t+2} \\ R_{t-2} & \longrightarrow & R_{t-2} + R_{t+2} \\ & \vdots & \\ R_7 & \longrightarrow & R_7 + R_{t+2} \\ R_5 & \longrightarrow & R_5 + R_{t+2} \end{array} \right.$$

$$R_2 \longrightarrow R_2 + R_{t+2}.$$

In addition, if

$$\left\{ \begin{array}{l} t \equiv 1 \pmod 4, \text{ then } R_1 \longrightarrow R_1 + R_{t+3}, \\ t \equiv 3 \pmod 4, \text{ then } R_1 \longrightarrow R_1 + R_{t+2}. \end{array} \right.$$

When applied in chronological order, this collection of row and column operations transforms the $(t+3) \times (t+3)$ block in the upper right corner of

$\mathbf{M_e}$ into

$$\mathbf{B} = \begin{bmatrix} 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & \cdots & 0 & 1 & 0 & \beta \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & \cdots & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & \cdots & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & \cdots & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & \cdots & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & \cdots & 1 & 1 & 1 & 1 \\ \vdots & \vdots & \vdots & & & \ddots & \ddots & \ddots & & & \vdots & \vdots & \vdots \\ \vdots & \vdots & \vdots & & & & \ddots & \ddots & \ddots & & \vdots & \vdots & \vdots \\ \vdots & \vdots & \vdots & & & & & \ddots & \ddots & \ddots & \vdots & \vdots & \vdots \\ \vdots & \vdots & \vdots & & & & & & \ddots & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & 0 & 0 & 0 & 0 \end{bmatrix},$$

while leaving the remaining elements in $\mathbf{M_e}$ unchanged. Furthermore, by applying the row operations

$$\begin{array}{rcl} R_3 & \longrightarrow & R_3 + R_4 \\ R_4 & \longrightarrow & R_4 + R_5 \\ & \vdots & \\ R_{t-1} & \longrightarrow & R_{t-1} + R_t \\ R_t & \longrightarrow & R_t + R_{t+1} \end{array}$$

$$R_2 \longrightarrow R_2 + (R_{t+1} + R_{t-1} + R_{t-3} + \cdots + R_6 + R_4 + R_1)$$

to $\mathbf{M_e}$ in the order listed above, $\mathbf{B}$ becomes

$$\mathbf{B}' = \begin{bmatrix} 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & \cdots & 0 & 1 & 0 & \beta \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \cdots & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & \cdots & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & \cdots & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & \cdots & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & \cdots & 0 & 0 & 0 & 1 \\ \vdots & \vdots & \vdots & & & \ddots & \ddots & \ddots & & & & \vdots & \vdots \\ \vdots & \vdots & \vdots & & & & \ddots & \ddots & \ddots & & & \vdots & \vdots \\ \vdots & \vdots & \vdots & & & & & \ddots & \ddots & \ddots & & \vdots & \vdots \\ \vdots & \vdots & \vdots & & & & & & \ddots & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & 0 & 0 & 0 & 0 \end{bmatrix}.$$

Note that these operations do not alter the other three blocks within $\mathbf{M_e}$. Next, we perform numerous row interchanges in sequential order:

$$\begin{array}{rcl}
R_{t+2} & \longleftrightarrow & R_{t+1} \\
R_{t+1} & \longleftrightarrow & R_{t} \\
 & \vdots & \\
R_{6} & \longleftrightarrow & R_{5} \\
R_{5} & \longleftrightarrow & R_{4} \\
R_{4} & \longleftrightarrow & R_{3} \\
R_{3} & \longleftrightarrow & R_{1} \\
R_{2} & \longleftrightarrow & R_{1} \\
R_{1} & \longleftrightarrow & R_{t+3}.
\end{array}$$

These row interchanges transform $\mathbf{M_e}$ into

$$\mathbf{M_e^*} = \left[\begin{array}{ccccccc|c}
0 & 0 & 0 & 0 & 0 & \cdots & 0 & \\
0 & 0 & 0 & 0 & 0 & \cdots & 0 & \\
0 & 0 & 0 & 0 & 0 & \cdots & 0 & \\
0 & 0 & 1 & 0 & 0 & \cdots & 0 & \mathbf{B}'' \\
0 & 0 & 0 & 0 & 0 & \cdots & 0 & \\
\vdots & & & & & \ddots & \vdots & \\
0 & 1 & 0 & 0 & \cdots & \cdots & 0 & \\
\hline
\multicolumn{7}{c|}{\mathbf{A}^T + \mathbf{D_2}} & \mathbf{D_{-1}}
\end{array}\right],$$

where

$$\mathbf{B}'' = \left[\begin{array}{ccccccccccccc}
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \cdots & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & \cdots & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & \cdots & 0 & 1 & 0 & \beta \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & \cdots & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & \cdots & 0 & 0 & 0 & 1 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & \cdots & 0 & 0 & 0 & 1 \\
\vdots & & & & & \ddots & \ddots & \ddots & & & & \vdots & \vdots \\
\vdots & & & & & & \ddots & \ddots & \ddots & & & \vdots & \vdots \\
\vdots & & & & & & & \ddots & \ddots & \ddots & & \vdots & \vdots \\
\vdots & & & & & & & & \ddots & \ddots & \ddots & \vdots & \vdots \\
\vdots & & & & & & & & & \ddots & 1 & 0 & 1 \\
\vdots & & & & & & & & & & 0 & 1 & 1 \\
0 & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & 0 & 0 & 1
\end{array}\right].$$

Our goal is to transform the $\mathbf{A}^T + \mathbf{D_2}$ block of $\mathbf{M}_\mathbf{e}^*$ into an upper triangular matrix. To accomplish this, we apply the following column replacements in $\mathbf{M}_\mathbf{e}^*$:

$$\begin{array}{rcl} C_{t+2} & \longrightarrow & C_{t+2} + C_{t+1} \\ C_{t+1} & \longrightarrow & C_{t+1} + C_t \\ & \vdots & \\ C_3 & \longrightarrow & C_3 + C_2 \\ C_2 & \longrightarrow & C_2 + C_1. \end{array}$$

These operations affect both the upper left and lower left blocks within $\mathbf{M}_\mathbf{e}^*$, changing this matrix into

$$\mathbf{M}_\mathbf{e}^{**} = \left[\begin{array}{cccccccccc|c}
0 & 0 & 0 & 0 & 0 & \cdots & \cdots & \cdots & \cdots & 0 & \\
0 & 0 & 0 & 0 & 0 & & & & & \vdots & \\
0 & 0 & 0 & 0 & 0 & & & & & \vdots & \\
0 & 0 & 1 & 1 & 0 & & & & & \vdots & \\
0 & 0 & 0 & 0 & 0 & & & & & \vdots & \\
\vdots & \vdots & \vdots & \vdots & & \ddots & & & & \vdots & \mathbf{B}'' \\
\vdots & \vdots & \vdots & \vdots & & & \ddots & & & \vdots & \\
0 & 0 & 0 & 0 & & & & 0 & 0 & 0 & \\
0 & 0 & 0 & 0 & \cdots & \cdots & \cdots & 0 & 0 & 0 & \\
0 & 1 & 1 & 0 & \cdots & \cdots & \cdots & 0 & 0 & 0 & \\
\hline
\beta & (\beta+1) & 0 & 0 & 1 & 1 & \cdots & \cdots & 1 & 1 & \\
1 & 1 & 1 & 0 & 0 & 0 & \cdots & \cdots & 0 & 1 & \\
1 & 0 & 1 & 0 & 0 & 0 & \cdots & \cdots & 0 & 0 & \\
1 & 0 & 0 & 1 & 0 & 0 & & & \vdots & \vdots & \\
0 & 1 & 0 & 0 & 1 & 0 & & & \vdots & \vdots & \\
1 & 0 & 0 & 0 & 0 & 1 & & & \vdots & \vdots & \mathbf{D_{-1}} \\
\vdots & \vdots & \vdots & \vdots & & & \ddots & & \vdots & \vdots & \\
\vdots & \vdots & \vdots & \vdots & & & & 1 & 0 & 0 & \\
0 & 1 & 0 & 0 & \cdots & \cdots & \cdots & 0 & 1 & 0 & \\
1 & 0 & 0 & 0 & \cdots & \cdots & \cdots & 0 & 0 & 0 &
\end{array}\right].$$

We then perform the following set of operations on $\mathbf{M_e^{**}}$.

$$\begin{array}{rcl}
C_2 & \longrightarrow & C_2 + (C_{t+2} + C_t + C_{t-2} + \cdots + C_7 + C_5) \\
C_1 & \longleftrightarrow & C_{t+3} \\
C_1 & \longrightarrow & C_1 + C_2 \\
R_{t+4} & \longrightarrow & R_{t+4} + R_1 \\
R_{t+5} & \longrightarrow & R_{t+5} + R_2.
\end{array}$$

Altogether, these five operations reduce the lower left block in $\mathbf{M_e^{**}}$ to an upper triangular matrix while transforming the lower right block into the identity matrix of order $(t+3)$. This yields

$$\mathbf{M_e^{***}} = \left[\begin{array}{c|c} \mathbf{G} & \mathbf{B''} \\ \hline \mathbf{H} & \mathbf{I_{t+3}} \end{array}\right],$$

where

$$\mathbf{G} = \begin{bmatrix}
0 & 0 & 0 & 0 & 0 & \cdots & \cdots & \cdots & 0 \\
0 & 0 & 0 & 0 & 0 & & & & \vdots \\
0 & 0 & 0 & 0 & 0 & & & & \vdots \\
0 & 0 & 1 & 1 & 0 & & & & \vdots \\
0 & 0 & 0 & 0 & 0 & & & & \vdots \\
\vdots & \vdots & \vdots & \vdots & & \ddots & & & \vdots \\
0 & 0 & 0 & 0 & & & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & \cdots & \cdots & 0 & 0 & 0 \\
1 & 1 & 1 & 0 & \cdots & \cdots & 0 & 0 & 0
\end{bmatrix},$$

and

$$\mathbf{H} = \begin{bmatrix}
1 & 0 & 0 & 0 & 1 & 1 & \cdots & \cdots & \cdots & 1 & \beta \\
0 & 1 & 1 & 0 & 0 & 0 & \cdots & \cdots & \cdots & 0 & 1 \\
0 & 0 & 1 & 0 & 0 & 0 & & & & 0 & 1 \\
0 & 0 & 0 & 1 & 0 & 0 & & & & 0 & 1 \\
0 & 0 & 0 & 0 & 1 & 0 & & & & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 & \ddots & & & 0 & 1 \\
\vdots & \vdots & & & & \ddots & \ddots & \ddots & & \vdots & \vdots \\
\vdots & \vdots & & & & & \ddots & 1 & 0 & 0 & 0 \\
\vdots & \vdots & & & & & & 0 & 1 & 0 & 1 \\
0 & 0 & \cdots & \cdots & \cdots & \cdots & \cdots & 0 & 0 & 1 & 0 \\
0 & 0 & \cdots & \cdots & \cdots & \cdots & \cdots & 0 & 0 & 0 & 1
\end{bmatrix}.$$

Finally, we apply Proposition 2.28 to $\mathbf{M_e^{***}}$ to obtain

$$\det(\mathbf{M_e^{***}}) = \det(\mathbf{I_{t+3}})\det(\mathbf{G} - \mathbf{B''}\mathbf{I_{t+3}^{-1}}\mathbf{H}).$$

Therefore,

$$\det(\mathbf{M_e^{***}}) = \det \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & \cdots & 1 & 1 & 1 & \beta \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & \cdots & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & \cdots & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & \cdots & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & \cdots & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & \cdots & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & \cdots & 0 & 0 & 0 & 1 \\ \vdots & \vdots & \vdots & \vdots & \vdots & & & \ddots & & & & \vdots & \vdots \\ \vdots & \vdots & \vdots & \vdots & \vdots & & & & \ddots & & & \vdots & \vdots \\ \vdots & \vdots & \vdots & \vdots & \vdots & & & & & \ddots & & \vdots & \vdots \\ \vdots & \vdots & \vdots & \vdots & \vdots & & & & & & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & \cdots & \cdots & \cdots & \cdots & \cdots & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & \cdots & \cdots & \cdots & \cdots & \cdots & 0 & 0 & 1 \end{bmatrix}.$$

Notice that the entries appearing in the middle of the third row and the middle of the last column of the above $(t+3) \times (t+3)$ matrix alternate between ones and zeros. To easily compute this determinant, we apply the following operations to the matrix above to reduce it to an upper triangular matrix with ones along its diagonal.

$$\begin{aligned} R_{t+3} &\longrightarrow R_{t+3} + R_2 \\ C_3 &\longleftrightarrow C_4 \\ R_1 &\longleftrightarrow R_{t+3} \\ R_{t+3} &\longrightarrow R_{t+3} + (R_1 + R_5 + R_6 + R_7 + \cdots + R_{t+1} + R_{t+2}). \end{aligned}$$

Since we are working over $\mathbb{F}_2$, the determinant of this upper triangular matrix is equal to that of $\mathbf{M_e^{***}}$. Therefore,

$$\det(\mathbf{M_e}) = \det(\mathbf{M_e^{***}}) = 1,$$

so $\mathbf{M_e}$ has full rank. Thus, by Equation (3.15), $s(n) = 0$ and n is a non-congruent number. □

4.3 Numerical Examples

The purpose of this section is to give some examples of non-congruent numbers generated by Theorem 4.1. The prime divisors of these numbers are required to satisfy certain Legendre symbols conditions, and hence Dirichlet's theorem on primes in arithmetic progressions (Theorem 2.20) guarantees that our theorem produces infinitely many non-congruent numbers. We list examples of non-congruent numbers described by Theorem 4.1 in the following table.

Table 4.1: Non-congruent numbers generated by Theorem 4.1

$n = 2pqrs_1s_2\cdots s_t$	$t \pmod 4$
$2\cdot 41\cdot 13\cdot 19\cdot 71\cdot 31\cdot 1319\cdot 743\cdot 3191\cdot 28151\cdot 52879\cdot 33287\cdot 160583$	1
$2\cdot 73\cdot 5\cdot 83\cdot 47\cdot 223\cdot 7927\cdot 2287\cdot 6247\cdot 7127\cdot 8647\cdot 26863\cdot 252463$	1
$2\cdot 17\cdot 5\cdot 3\cdot 23\cdot 263\cdot 503\cdot 1583\cdot 743\cdot 18143\cdot 18047$	3
$2\cdot 17\cdot 29\cdot 131\cdot 31\cdot 127\cdot 743\cdot 967\cdot 2207\cdot 3391\cdot 2879$ $\cdot 59671\cdot 118247\cdot 350447\cdot 1378439$	3

In Appendix A, we show how Maple can be used to generate non-congruent numbers, such as the ones listed in Table 4.1, satisfying the conditions imposed in Theorem 4.1.

Chapter 5

The Generation of Families of Odd Non-congruent Numbers From Known Non-congruent Numbers

5.1 Overview

In this chapter, we present a novel technique for generating families of odd non-congruent numbers. Unlike other known results on non-congruent numbers that impose congruence conditions on each prime factor of a non-congruent number and on the Legendre symbols relating these primes, the new technique described in this chapter provides a general approach for finding families of non-congruent numbers. That is, given an odd non-congruent number α corresponding to a congruent number elliptic curve with 2-Selmer rank equal to zero, new non-congruent numbers can be constructed by multiplying α by primes of a specified form. This process allows existing families of non-congruent numbers to be extended and infinitely many non-congruent numbers to be produced.

This chapter is based on results that appear in [41] and [44].

5.2 Extending Known Families of Odd Non-congruent Numbers

This section provides an introduction to our extension technique for generating new families of non-congruent numbers. We begin by introducing some notation.

Let $p_i \equiv 5 \pmod 8$ and $q_j \equiv 3 \pmod 8$ with $i, j \in \mathbb{N}^+$ be distinct odd primes, and let $a, b \in \mathbb{N}$ with $(a + b) > 0$. We define the sets

$$P = \begin{cases} \emptyset & \text{if } a = 0, \\ \{p_1, p_2, \ldots, p_a\} & \text{if } a > 0, \end{cases}$$

and

$$Q = \begin{cases} \emptyset & \text{if } b = 0, \\ \{q_1, q_2, \ldots, q_b\} & \text{if } b > 0. \end{cases}$$

We now state the following theorem from [41].

Theorem 5.1. *Let*

$$\alpha = \left(\prod_{p_i \in P} p_i\right)\left(\prod_{q_j \in Q} q_j\right),$$

and suppose that the elliptic curve

$$y^2 = x(x^2 - \alpha^2)$$

has $s(\alpha) = 0$. Define the square-free positive integer n by

$$n = \alpha r_1 r_2 \cdots r_v,$$

where $r_1, r_2, \ldots, r_v$ are primes satisfying $r_k \equiv 1 \pmod 8$ for all $k \in [1, v]$ with $v \in \mathbb{N}^+$. If for each k with $1 \leq k \leq v$ the set S_k defined by

$$S_k = \left\{ \left(\frac{r_k}{p_i}\right), \left(\frac{r_k}{q_j}\right), \left(\frac{r_k}{r_h}\right) \text{ with } 1 \leq i \leq a,\ 1 \leq j \leq b,\ \text{and } 1 \leq h < k \leq v \right\}$$

contains exactly one Legendre symbol equal to -1, then $s(n) = 0$ and n is a non-congruent number.

Proof. We work over $\mathbb{F}_2$ and use properties from the field of linear algebra in conjunction with Monsky's formula for the 2-Selmer rank of E_n to prove this result. We use Equation (3.16) to construct the $(2a + 2b) \times (2a + 2b)$ Monsky matrix for $\alpha = p_1 p_2 \cdots p_a q_1 q_2 \cdots q_b$. This matrix has the form

$$\mathbf{M}_\alpha = \left[\begin{array}{c|c} \mathbf{A}_\alpha + \mathbf{D}^\alpha_\mathbf{2} & \mathbf{I_{a+b}} \\ \hline \mathbf{I_{a+b}} & \mathbf{A}_\alpha + \mathbf{D}^\alpha_\mathbf{-2} \end{array}\right], \tag{5.1}$$

where

$$\mathbf{D}^\alpha_\mathbf{2} = \mathbf{I_{a+b}} \qquad \text{and} \qquad \mathbf{D}^\alpha_\mathbf{-2} = \left[\begin{array}{c|c} \mathbf{I_a} & \mathbf{0} \\ \hline \mathbf{0} & \mathbf{0_b} \end{array}\right]$$

represent the diagonal matrices for α, and $\mathbf{A}_\alpha$ is the square $\mathbf{A}$ matrix of order $(a + b)$ corresponding to α. We use the specified Legendre symbol conditions imposed on the prime divisors of $n = \alpha r_1 r_2 \cdots r_v$ and Equation (3.14) to form the $\mathbf{A}$ matrix for n, denoted by $\mathbf{A_n}$. As a result, the Monsky matrix for n can be written as

$$\mathbf{M_n} = \left[\begin{array}{c|c} \mathbf{A_n} + \mathbf{D_2^n} & \mathbf{D_2^n} \\ \hline \mathbf{D_2^n} & \mathbf{A_n} + \mathbf{D_{-2}^n} \end{array}\right],$$

where

$$\mathbf{D_2^n} = \left[\begin{array}{c|c} \mathbf{D_2^\alpha} & \mathbf{0} \\ \hline \mathbf{0} & \mathbf{0_v} \end{array}\right] \qquad \text{and} \qquad \mathbf{D_{-2}^n} = \left[\begin{array}{c|c} \mathbf{D_{-2}^\alpha} & \mathbf{0} \\ \hline \mathbf{0} & \mathbf{0_v} \end{array}\right].$$

Guided by the structure of the matrix $\mathbf{A_n}$, we use elementary row and column operations to reduce $\mathbf{M_n}$ until the value of its determinant can be easily computed. Since we are working over $\mathbb{F}_2$, the operations yield a matrix with the same determinant. To describe the sequence of steps used to reduce $\mathbf{M_n}$, we let m_{ij} denote the entry in the i^{th} row and j^{th} column of $\mathbf{M_n}$. We consider those entries with $m_{ij} = 1$, where $1 \leq i \leq (a + b + v)$, $(a+b) < j \leq (a+b+v)$, and $i < j$. Note that for every $j \in [a+b+1, a+b+v]$, there exists a single value of $i \in [1, a + b + v]$ satisfying $m_{ij} = 1$. Therefore, beginning with $j = (a+b+v)$, we determine the corresponding value of i for which $m_{ij} = 1$. We subtract column j from column i, and then subtract row j from row i. Following this, we decrease the value of j by one and repeat the previously described column and row subtraction operations. We continue this process for each $j = (a+b+v-1), (a+b+v-2), \ldots, (a+b+1)$. Upon completing the v column subtractions and v row subtractions, we find that the upper left block of $\mathbf{M_n}$ is reduced to

$$\left[\begin{array}{c|c} \mathbf{A}_\alpha + \mathbf{D_2^\alpha} & \mathbf{0} \\ \hline \mathbf{0} & \mathbf{I_v} \end{array}\right],$$

while the remaining three blocks in $\mathbf{M_n}$ are left unaltered.

The structure of the original $\mathbf{A_n} + \mathbf{D_2^n}$ and $\mathbf{A_n} + \mathbf{D_{-2}^n}$ blocks in $\mathbf{M_n}$ is similar, so for each $j \in [2a + 2b + v + 1, 2a + 2b + 2v]$, there is precisely one value of $i \in [a + b + v + 1, 2a + 2b + 2v]$ for which $m_{ij} = 1$. Therefore, we repeat the aforementioned procedure, but with the rows i and the columns j satisfying $(a+b+v+1) \leq i \leq (2a+2b+2v)$, $(2a+2b+v) < j \leq (2a+2b+2v)$, and $i < j$. We begin with $j = (2a + 2b + 2v)$ and complete the necessary v

column subtractions and v row subtractions, thus reducing the lower right block of $\mathbf{M_n}$ to

$$\left[\begin{array}{c|c} \mathbf{A}_{\alpha} + \mathbf{D}^{\alpha}_{-\mathbf{2}} & \mathbf{0} \\ \hline \mathbf{0} & \mathbf{I_v} \end{array}\right].$$

Altogether, these operations transform $\mathbf{M_n}$ into

$$\mathbf{M}^{*}_{\mathbf{n}} = \left[\begin{array}{c|c||c|c} \mathbf{A}_{\alpha} + \mathbf{D}^{\alpha}_{\mathbf{2}} & \mathbf{0} & \mathbf{I_{a+b}} & \mathbf{0} \\ \hline \mathbf{0} & \mathbf{I_v} & \mathbf{0} & \mathbf{0} \\ \hline\hline \mathbf{I_{a+b}} & \mathbf{0} & \mathbf{A}_{\alpha} + \mathbf{D}^{\alpha}_{-\mathbf{2}} & \mathbf{0} \\ \hline \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{I_v} \end{array}\right].$$

We now add rows $(2a+2b+v+1)$ through $(2a+2b+2v)$ to rows $(a+b+1)$ through $(a+b+v)$ respectively to get

$$\mathbf{M}^{**}_{\mathbf{n}} = \left[\begin{array}{c||c} \begin{array}{c|c} \mathbf{A}_{\alpha} + \mathbf{D}^{\alpha}_{\mathbf{2}} & \mathbf{0} \\ \hline \mathbf{0} & \mathbf{I_v} \end{array} & \mathbf{I_{a+b+v}} \\ \hline\hline \mathbf{D}^{\mathbf{n}}_{\mathbf{2}} & \begin{array}{c|c} \mathbf{A}_{\alpha} + \mathbf{D}^{\alpha}_{-\mathbf{2}} & \mathbf{0} \\ \hline \mathbf{0} & \mathbf{I_v} \end{array} \end{array}\right].$$

Following this, we perform $(a+b+v)$ row interchanges to $\mathbf{M}^{**}_{\mathbf{n}}$ to obtain the matrix

$$\mathbf{M}^{***}_{\mathbf{n}} = \left[\begin{array}{c||c} \mathbf{D}^{\mathbf{n}}_{\mathbf{2}} & \begin{array}{c|c} \mathbf{A}_{\alpha} + \mathbf{D}^{\alpha}_{-\mathbf{2}} & \mathbf{0} \\ \hline \mathbf{0} & \mathbf{I_v} \end{array} \\ \hline\hline \begin{array}{c|c} \mathbf{A}_{\alpha} + \mathbf{D}^{\alpha}_{\mathbf{2}} & \mathbf{0} \\ \hline \mathbf{0} & \mathbf{I_v} \end{array} & \mathbf{I_{a+b+v}} \end{array}\right].$$

Note that since we are working over $\mathbb{F}_2$,

$$\det(\mathbf{M_n}) = \det(\mathbf{M}^{*}_{\mathbf{n}}) = \det(\mathbf{M}^{**}_{\mathbf{n}}) = \det(\mathbf{M}^{***}_{\mathbf{n}}). \tag{5.2}$$

Applying Proposition 2.28 to $\mathbf{M}^{***}_{\mathbf{n}}$ allows us to deduce that its determinant is equal to

$$\det(\mathbf{I_{a+b+v}})\det\left(\mathbf{D}^{\mathbf{n}}_{\mathbf{2}} - \left[\begin{array}{c|c} \mathbf{A}_{\alpha} + \mathbf{D}^{\alpha}_{-\mathbf{2}} & \mathbf{0} \\ \hline \mathbf{0} & \mathbf{I_v} \end{array}\right] \mathbf{I}^{-\mathbf{1}}_{\mathbf{a+b+v}} \left[\begin{array}{c|c} \mathbf{A}_{\alpha} + \mathbf{D}^{\alpha}_{\mathbf{2}} & \mathbf{0} \\ \hline \mathbf{0} & \mathbf{I_v} \end{array}\right]\right),$$

which, when simplified, reduces to

$$\begin{aligned}
\det(\mathbf{M}_{\mathbf{n}}^{***}) &= \det\left(\left[\begin{array}{c|c} \mathbf{I}_{\mathbf{a+b}} & \mathbf{0} \\ \hline \mathbf{0} & \mathbf{0} \end{array}\right] - \left[\begin{array}{c|c} (\mathbf{A}_\alpha + \mathbf{D}^{\alpha}_{\mathbf{-2}})(\mathbf{A}_\alpha + \mathbf{D}^{\alpha}_{\mathbf{2}}) & \mathbf{0} \\ \hline \mathbf{0} & \mathbf{I}_{\mathbf{v}} \end{array}\right]\right) \\
&= \det\left(\mathbf{I}_{\mathbf{a+b}} - \left(\mathbf{A}_\alpha + \mathbf{D}^{\alpha}_{\mathbf{-2}}\right)\left(\mathbf{A}_\alpha + \mathbf{D}^{\alpha}_{\mathbf{2}}\right)\right) \det\left(\mathbf{I}_{\mathbf{v}}\right) \\
&= \det\left(\mathbf{I}_{\mathbf{a+b}} - \left(\mathbf{A}_\alpha + \mathbf{D}^{\alpha}_{\mathbf{-2}}\right)\left(\mathbf{A}_\alpha + \mathbf{D}^{\alpha}_{\mathbf{2}}\right)\right). \qquad (5.3)
\end{aligned}$$

To compute this determinant, we need to consider the matrix $\mathbf{M}_\alpha$ described by Equation (5.1). By assumption $s(\alpha) = 0$, so Equation (3.15) implies that $\mathbf{M}_\alpha$ has full rank, and hence

$$\det(\mathbf{M}_\alpha) \neq 0. \qquad (5.4)$$

In addition, if we perform $(a + b)$ row interchanges to $\mathbf{M}_\alpha$ to transform it into

$$\mathbf{M}^*_\alpha = \left[\begin{array}{c|c} \mathbf{I}_{\mathbf{a+b}} & \mathbf{A}_\alpha + \mathbf{D}^{\alpha}_{\mathbf{-2}} \\ \hline \mathbf{A}_\alpha + \mathbf{D}^{\alpha}_{\mathbf{2}} & \mathbf{I}_{\mathbf{a+b}} \end{array}\right],$$

and apply Proposition 2.28 to $\mathbf{M}^*_\alpha$, then

$$\begin{aligned}
\det\left(\mathbf{M}_\alpha\right) = \det\left(\mathbf{M}^*_\alpha\right) &= \det\left(\mathbf{I}_{\mathbf{a+b}}\right)\det\left(\mathbf{I}_{\mathbf{a+b}} - \left(\mathbf{A}_\alpha + \mathbf{D}^{\alpha}_{\mathbf{-2}}\right)\mathbf{I}^{\mathbf{-1}}_{\mathbf{a+b}}\left(\mathbf{A}_\alpha + \mathbf{D}^{\alpha}_{\mathbf{2}}\right)\right) \\
&= \det\left(\mathbf{I}_{\mathbf{a+b}} - \left(\mathbf{A}_\alpha + \mathbf{D}^{\alpha}_{\mathbf{-2}}\right)\left(\mathbf{A}_\alpha + \mathbf{D}^{\alpha}_{\mathbf{2}}\right)\right). \qquad (5.5)
\end{aligned}$$

Combining Equations (5.2), (5.3), (5.4), and (5.5) enables us to conclude that

$$\det(\mathbf{M}_{\mathbf{n}}) \neq 0.$$

Thus, $s(n) = 0$ and n is a non-congruent number. □

5.3 Numerical Examples of Odd Non-congruent Numbers

In this section, we provide examples to demonstrate how Theorem 5.1 can be used to generate new non-congruent numbers from known families of non-congruent numbers. Because these numbers are specified by conditions on the Legendre symbol relating their prime factors, Dirichlet's theorem on primes in arithmetic progressions (Theorem 2.20) guarantees that infinitely many non-congruent numbers are produced by Theorem 5.1. Also, note that the examples we list in Table 5.1 clearly belong to new families of non-congruent numbers because their prime factorizations differ from those of existing families of non-congruent numbers [2, 6, 11–13, 15–17, 24, 27, 28, 36, 37, 39, 40, 49, 58].

We begin by extending Iskra's family of non-congruent numbers [24].

Theorem 5.2 (**Iskra**). *Let $a \in \mathbb{N}^+$ and suppose that $p_1, p_2, \ldots, p_a$ are distinct primes satisfying $p_i \equiv 3 \pmod 8$ and $\left(\frac{p_j}{p_i}\right) = -1$ for $j < i$. Then $\alpha = p_1 p_2 \cdots p_a$ is a non-congruent number.*

In Reinholz's master's thesis [38, Section 4.2], the congruent number elliptic curves associated with numbers described by Iskra's theorem are shown to have 2-Selmer rank of zero. As a result, new non-congruent numbers can be produced by using Theorem 5.1 to append a tail of primes of the form $8k+1$ to Iskra's non-congruent numbers.

Next, we apply Theorem 5.1 to the following result by Reinholz et al. [39].

Theorem 5.3 (**Reinholz et al.**). *Let m be a fixed nonnegative even integer and let a be any positive integer satisfying $a \geq m$. Let N_m denote the set of positive integers with prime factorization $p_1 p_2 \cdots p_a$, where $p_1, p_2, \ldots, p_a$ are distinct primes of the form $8k+3$ such that*

$$\left(\frac{p_j}{p_i}\right) = \begin{cases} -1 & \text{if } 1 \leq j < i \text{ and } (j,i) \neq (1,m), \\ 1 & \text{if } 1 \leq j < i \text{ and } (j,i) = (1,m). \end{cases}$$

If $\alpha \in N_m$, then α is non-congruent.

In the proof of this theorem [39], the congruent number elliptic curves corresponding to these non-congruent numbers are shown to have 2-Selmer rank equal to zero. Therefore, Theorem 5.1 can be directly applied to Theorem 5.3 to generate infinitely many new non-congruent numbers.

Finally, we use Theorem 5.1 to extend an important result by Ouyang and Zhang [37].

Theorem 5.4 (**Ouyang and Zhang**). *Let*

$$\left[\frac{x}{h}\right] = \frac{\left(1 - \left(\frac{x}{h}\right)\right)}{2},$$

and suppose that $\alpha = p_1 p_2 \cdots p_k \equiv 1, 3 \pmod 8$ with $p_i \equiv \pm 3 \pmod 8$ for all $i \in [1,k]$. Define $\mathbf{B}$ to be the $k \times k$ matrix with (i,j)-entries $\left[\frac{p_j}{p_i}\right]$ for $i \neq j$ and with (i,i)-entries $\left[\frac{\alpha/p_i}{p_i}\right]$, and

$$\mathbf{C} = \operatorname{diag}\left\{\left[\frac{-1}{p_1}\right], \left[\frac{-1}{p_2}\right], \ldots, \left[\frac{-1}{p_k}\right]\right\}.$$

If $\mathbf{B}^2 + \mathbf{CB} + \mathbf{C}$ *is invertible, then* α *is a non-congruent number.*

With a little effort, one can prove that for the integer α in Theorem 5.4, the condition that $\mathbf{B}^2 + \mathbf{CB} + \mathbf{C}$ is invertible is equivalent to the Monsky matrix having full rank. Thus, the matrix $\mathbf{B}^2 + \mathbf{CB} + \mathbf{C}$ is invertible if and only if $s(\alpha) = 0$. As a result, Theorem 5.1 can be used to extend Ouyang and Zhang's work and generate new non-congruent numbers containing arbitrarily many prime factors belonging to two or three odd congruence classes modulo eight.

Numerical examples obtained by applying Theorem 5.1 to the non-congruent numbers in Theorems 5.2-5.4 are given in Table 5.1.

Table 5.1: Non-congruent numbers generated by Theorem 5.1

Theorem Satisfied by $\boldsymbol{\alpha}$	$\boldsymbol{n = (\alpha) \cdot r_1 r_2 \cdots r_k}$	**Extension Tail Legendre Symbols that Equal -1**
Theorem 5.2	$(19 \cdot 11 \cdot 163 \cdot 419) \cdot 97 \cdot 313 \cdot 617 \cdot 1697 \cdot 1721 \cdot 6521 \cdot 15361 \cdot 16889$	$\left(\frac{97}{19}\right), \left(\frac{313}{419}\right), \left(\frac{617}{163}\right), \left(\frac{1697}{163}\right), \left(\frac{1721}{1697}\right), \left(\frac{6521}{1721}\right), \left(\frac{15361}{419}\right), \left(\frac{16889}{1721}\right)$
Theorem 5.2	$(347 \cdot 83 \cdot 11 \cdot 3 \cdot 499 \cdot 1123 \cdot 2803) \cdot 673 \cdot 2953 \cdot 3617 \cdot 7417 \cdot 8713$	$\left(\frac{673}{11}\right), \left(\frac{2953}{1123}\right), \left(\frac{3617}{3}\right), \left(\frac{7417}{1123}\right), \left(\frac{8713}{2953}\right)$
Theorem 5.3	$(11 \cdot 59 \cdot 163 \cdot 307 \cdot 947) \cdot 41 \cdot 1361 \cdot 2017 \cdot 4057 \cdot 4673 \cdot 8969$	$\left(\frac{41}{11}\right), \left(\frac{1361}{11}\right), \left(\frac{2017}{59}\right), \left(\frac{4057}{947}\right), \left(\frac{4673}{163}\right), \left(\frac{8969}{4673}\right)$
Theorem 5.3	$(3 \cdot 11 \cdot 67 \cdot 163 \cdot 691 \cdot 1483 \cdot 3019 \cdot 2179 \cdot 16987) \cdot 2137 \cdot 4273 \cdot 13553 \cdot 36793$	$\left(\frac{2137}{163}\right), \left(\frac{4273}{67}\right), \left(\frac{13553}{3}\right), \left(\frac{36793}{1483}\right)$
Theorem 5.4	$(3 \cdot 11 \cdot 19 \cdot 43 \cdot 59 \cdot 5 \cdot 13 \cdot 29 \cdot 37) \cdot 27481 \cdot 31321 \cdot 52561 \cdot 78049$	$\left(\frac{27481}{29}\right), \left(\frac{31321}{37}\right), \left(\frac{52561}{13}\right), \left(\frac{78049}{29}\right)$
Theorem 5.4	$(3 \cdot 19 \cdot 67 \cdot 83 \cdot 13 \cdot 61 \cdot 101 \cdot 149) \cdot 4177 \cdot 9649 \cdot 9721 \cdot 17449 \cdot 26953 \cdot 49297$	$\left(\frac{4177}{61}\right), \left(\frac{9649}{61}\right), \left(\frac{9721}{19}\right), \left(\frac{17449}{83}\right), \left(\frac{26953}{9721}\right), \left(\frac{49297}{67}\right)$

Note that the non-congruent numbers presented in Table 5.1 were constructed using similar Maple code to that described in Appendix A.

5.4 An Extension Technique for Generating New Families of Odd Non-congruent Numbers

In this section, we present a method for generating new families of odd non-congruent numbers by extending other known families of non-congruent numbers. Of significance is the fact that our method produces non-congruent numbers with arbitrarily many distinct prime divisors in each of the four odd congruence classes modulo eight. This is a distinguishing feature of our result, as all other existing theorems on non-congruent numbers impose restrictions on the number of prime factors belonging to the odd congruence classes modulo eight.

We introduce some notation that will be used throughout this section. Let p_i, q_j, r_k, and s_l with $i, j, k, l \in \mathbb{N}^+$ be distinct odd primes, and let $a, b, c, d \in \mathbb{N}$ with $(a + b + c + d) > 0$. We define the set

$$P = \begin{cases} \emptyset & \text{if } a = 0, \\ \{p_1, p_2, \ldots, p_a\} & \text{if } a > 0. \end{cases}$$

The sets Q, R, and S are defined analogously with $|Q| = b, |R| = c$, and $|S| = d$. In addition, we let

$$W = P \cup Q \cup R \cup S.$$

Our main result [44] provides a general extension technique for constructing new families of odd non-congruent numbers.

Theorem 5.5. *Define*

$$\alpha = \left(\prod_{p_i \in P} p_i\right)\left(\prod_{q_j \in Q} q_j\right)\left(\prod_{r_k \in R} r_k\right)\left(\prod_{s_l \in S} s_l\right), \tag{5.6}$$

and suppose that the elliptic curve

$$y^2 = x(x^2 - \alpha^2)$$

has 2-Selmer rank of zero. Let $t > d$ with $t \in \mathbb{N}^+$, and define the odd square-free positive integer n by

$$n = \alpha s_{d+1} s_{d+2} \cdots s_t,$$

where the prime factors of n satisfy the congruence conditions described in one of the three cases in Table 5.2.

Table 5.2: Congruence conditions for the prime factors of the odd number n

Condition	$\boldsymbol{p_i}$**(mod 8)** $\forall\, \boldsymbol{p_i \in P}$	$\boldsymbol{q_j}$**(mod 8)** $\forall\, \boldsymbol{q_j \in Q}$	$\boldsymbol{r_k}$**(mod 8)** $\forall\, \boldsymbol{r_k \in R}$	$\boldsymbol{s_\gamma}$**(mod 8)** $\forall\, \boldsymbol{\gamma \in [1, t]}$
I	1	5	7	3
II	1	7	3	5
III	5	3	7	1

In addition, assume that the primes appended onto α satisfy one of the following Legendre symbol conditions.

Condition 1:
For all $h \in [d+1, t]$, $p_i \in P$, $q_j \in Q$, $r_k \in R$, and $g \in [1, h)$, one of the following four sets of Legendre symbol conditions hold.

A) $$\left(\frac{s_h}{p_i}\right) = \left(\frac{s_h}{q_j}\right) = \left(\frac{s_h}{r_k}\right) = \left(\frac{s_h}{s_g}\right) = 1.$$

B) $$\left(\frac{p_i}{s_h}\right) = \left(\frac{q_j}{s_h}\right) = \left(\frac{r_k}{s_h}\right) = \left(\frac{s_g}{s_h}\right) = 1.$$

C) $$\left(\frac{s_h}{p_i}\right) = \left(\frac{s_h}{q_j}\right) = \left(\frac{s_h}{r_k}\right) = \left(\frac{s_h}{s_g}\right) = -1.$$

D) $$\left(\frac{p_i}{s_h}\right) = \left(\frac{q_j}{s_h}\right) = \left(\frac{r_k}{s_h}\right) = \left(\frac{s_g}{s_h}\right) = -1.$$

Condition 2:
For all $h, \beta \in [d+1, t]$ with $h \neq \beta$

$$\left(\frac{s_\beta}{s_h}\right) = 1,$$

and define $T \subseteq W$ with

$$T = \left\{\mu \,\middle|\, \left(\frac{s_h}{\mu}\right) = -1 \;\;\forall\;\; h \in [d+1, t]\right\}$$

and $|T| \equiv 1 \pmod 2$. For all primes $\varepsilon \in W \backslash T$,

$$\left(\frac{s_h}{\varepsilon}\right) = 1 \;\;\forall\;\; h \in [d+1, t].$$

Condition 3:
For each $h \in [d+1, t]$, the set L_h defined by

$$L_h = \left\{ \left(\frac{s_h}{p_i}\right), \left(\frac{s_h}{q_j}\right), \left(\frac{s_h}{r_k}\right), \left(\frac{s_h}{s_g}\right) \ \textit{with } p_i \in P, q_j \in Q, r_k \in R, g \in [1, h) \right\}$$

has exactly one Legendre symbol equal to -1.

Then, in each of the cases described in Table 5.3, n is a non-congruent number and the 2-Selmer rank of the elliptic curve $y^2 = x(x^2 - n^2)$ is zero.

Table 5.3: Conditions on the prime factors in the extension tail of the odd number n

	Case	**Congruence Condition**	**Legendre Symbol Condition**	**Parity of $(t - d)$**
Case I.1	I.1.A	I	1.A	No restriction
	I.1.B	I	1.B	No restriction
	I.1.C	I	1.C	Even
	I.1.D	I	1.D	Even
	II.2	II	2	Even
	III.2	III	2	Even
	III.3	III	3	No restriction

To prove this theorem, we use Monsky's formula for the 2-Selmer rank of E_n along with various properties of determinants, including the one described by the following lemma.

Lemma 5.6. *Let*

$$\mathbf{Q_1} = \begin{bmatrix} \mathbf{I_{n_1}} & \mathbf{0} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{I_{n_3}} & \mathbf{0} \\ \mathbf{0} & \mathbf{I_{n_2}} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{I_{n_4}} \end{bmatrix}, \qquad \mathbf{Q_2} = \begin{bmatrix} \mathbf{I_{n_1}} & \mathbf{0} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{I_{n_2}} & \mathbf{0} \\ \mathbf{0} & \mathbf{I_{n_3}} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{I_{n_4}} \end{bmatrix},$$

$$\mathbf{R_1} = \begin{bmatrix} \mathbf{I_{n_1}} & \mathbf{0} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{I_{n_3}} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{I_{n_4}} \\ \mathbf{0} & \mathbf{I_{n_2}} & \mathbf{0} & \mathbf{0} \end{bmatrix}, \quad \textit{and} \quad \mathbf{R_2} = \begin{bmatrix} \mathbf{I_{n_1}} & \mathbf{0} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{I_{n_2}} \\ \mathbf{0} & \mathbf{I_{n_3}} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{I_{n_4}} & \mathbf{0} \end{bmatrix},$$

where $n_1, n_2, n_3, n_4 \in \mathbb{N}^+$. Then

$$\mathbf{Q_1Q_2} = \mathbf{Q_2Q_1} = \mathbf{R_1R_2} = \mathbf{R_2R_1} = \mathbf{I_{n_1+n_2+n_3+n_4}}.$$

Define the square matrix $\mathbf{M}$ of order $(n_1 + n_2 + n_3 + n_4)$ by

$$\mathbf{M} = \begin{bmatrix} \mathbf{M_{11}} & \mathbf{M_{12}} & \mathbf{M_{13}} & \mathbf{M_{14}} \\ \mathbf{M_{21}} & \mathbf{M_{22}} & \mathbf{M_{23}} & \mathbf{M_{24}} \\ \mathbf{M_{31}} & \mathbf{M_{32}} & \mathbf{M_{33}} & \mathbf{M_{34}} \\ \mathbf{M_{41}} & \mathbf{M_{42}} & \mathbf{M_{43}} & \mathbf{M_{44}} \end{bmatrix},$$

where $\mathbf{M_{ij}}$ is a $n_i \times n_j$ matrix. Then

$$\mathbf{M}^\diamond = \mathbf{Q_1MQ_2} = \begin{bmatrix} \mathbf{M_{11}} & \mathbf{M_{13}} & \mathbf{M_{12}} & \mathbf{M_{14}} \\ \mathbf{M_{31}} & \mathbf{M_{33}} & \mathbf{M_{32}} & \mathbf{M_{34}} \\ \mathbf{M_{21}} & \mathbf{M_{23}} & \mathbf{M_{22}} & \mathbf{M_{24}} \\ \mathbf{M_{41}} & \mathbf{M_{43}} & \mathbf{M_{42}} & \mathbf{M_{44}} \end{bmatrix}, \tag{5.7}$$

$$\mathbf{M}^\blacktriangle = \mathbf{R_1MR_2} = \begin{bmatrix} \mathbf{M_{11}} & \mathbf{M_{13}} & \mathbf{M_{14}} & \mathbf{M_{12}} \\ \mathbf{M_{31}} & \mathbf{M_{33}} & \mathbf{M_{34}} & \mathbf{M_{32}} \\ \mathbf{M_{41}} & \mathbf{M_{43}} & \mathbf{M_{44}} & \mathbf{M_{42}} \\ \mathbf{M_{21}} & \mathbf{M_{23}} & \mathbf{M_{24}} & \mathbf{M_{22}} \end{bmatrix}, \tag{5.8}$$

$$\mathbf{M}^* = \mathbf{R_1MQ_2} = \begin{bmatrix} \mathbf{M_{11}} & \mathbf{M_{13}} & \mathbf{M_{12}} & \mathbf{M_{14}} \\ \mathbf{M_{31}} & \mathbf{M_{33}} & \mathbf{M_{32}} & \mathbf{M_{34}} \\ \mathbf{M_{41}} & \mathbf{M_{43}} & \mathbf{M_{42}} & \mathbf{M_{44}} \\ \mathbf{M_{21}} & \mathbf{M_{23}} & \mathbf{M_{22}} & \mathbf{M_{24}} \end{bmatrix}, \tag{5.9}$$

and

$$\mathbf{M}' = \mathbf{Q_1MR_2} = \begin{bmatrix} \mathbf{M_{11}} & \mathbf{M_{13}} & \mathbf{M_{14}} & \mathbf{M_{12}} \\ \mathbf{M_{31}} & \mathbf{M_{33}} & \mathbf{M_{34}} & \mathbf{M_{32}} \\ \mathbf{M_{21}} & \mathbf{M_{23}} & \mathbf{M_{24}} & \mathbf{M_{22}} \\ \mathbf{M_{41}} & \mathbf{M_{43}} & \mathbf{M_{44}} & \mathbf{M_{42}} \end{bmatrix}. \tag{5.10}$$

Thus, over $\mathbb{F}_2$,

$$\det(\mathbf{M}) = \det(\mathbf{M}^\diamond) = \det(\mathbf{M}^\blacktriangle) = \det(\mathbf{M}^*) = \det(\mathbf{M}').$$

The proofs of the separate cases in Theorem 5.5 are sufficiently different, so we provide details for each of them individually. Throughout the proofs, we work over the finite field $\mathbb{F}_2$ and let

$$\delta = (a + b + c) \qquad \text{and} \qquad \omega = (2\delta + t + d). \tag{5.11}$$

We also let $\mathbf{A}_\alpha$ denote the $(\delta + d) \times (\delta + d)$ $\mathbf{A}$ matrix for the integer α; the entries in this matrix are defined in Equation (3.14).

We begin by presenting the proof of the first four cases listed in Table 5.3.

Case I.1 Proof. Consider $n = \alpha s_{d+1} s_{d+2} \cdots s_t$ and recall the Monsky matrix described in Equation (3.16). We form the diagonal $\mathbf{D_2}$ and $\mathbf{D_{-2}}$ matrices corresponding to n; they can be written as

$$\mathbf{D_2^n} = \left[\begin{array}{c|c|c|c|c} \mathbf{0_a} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} \\ \hline \mathbf{0} & \mathbf{I_b} & \mathbf{0} & \mathbf{0} & \mathbf{0} \\ \hline \mathbf{0} & \mathbf{0} & \mathbf{0_c} & \mathbf{0} & \mathbf{0} \\ \hline \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{I_d} & \mathbf{0} \\ \hline \hline \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{I_{t-d}} \end{array}\right] = \left[\begin{array}{c|c} \mathbf{D_2^\alpha} & \mathbf{0} \\ \hline \mathbf{0} & \mathbf{I_{t-d}} \end{array}\right] \tag{5.12}$$

and

$$\mathbf{D_{-2}^n} = \left[\begin{array}{c|c|c|c} \mathbf{0_a} & \mathbf{0} & \mathbf{0} & \mathbf{0} \\ \hline \mathbf{0} & \mathbf{I_{b+c}} & \mathbf{0} & \mathbf{0} \\ \hline \mathbf{0} & \mathbf{0} & \mathbf{0_d} & \mathbf{0} \\ \hline \hline \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0_{t-d}} \end{array}\right] = \left[\begin{array}{c|c} \mathbf{D_{-2}^\alpha} & \mathbf{0} \\ \hline \mathbf{0} & \mathbf{0_{t-d}} \end{array}\right]. \tag{5.13}$$

We also define a pair of $(t - d) \times (\delta + d)$ matrices

$$\mathbf{T} = \left[\begin{array}{cccc} \underbrace{\begin{matrix} 0 & \cdots & 0 \\ \vdots & & \vdots \\ 0 & \cdots & 0 \end{matrix}}_{a \text{ columns}} & \underbrace{\begin{matrix} 0 & \cdots & 0 \\ \vdots & & \vdots \\ 0 & \cdots & 0 \end{matrix}}_{b \text{ columns}} & \underbrace{\begin{matrix} 1 & \cdots & 1 \\ \vdots & & \vdots \\ 1 & \cdots & 1 \end{matrix}}_{c \text{ columns}} & \underbrace{\begin{matrix} 1 & \cdots & 1 \\ \vdots & & \vdots \\ 1 & \cdots & 1 \end{matrix}}_{d \text{ columns}} \end{array}\right] \tag{5.14}$$

and

$$\mathbf{U} = \left[\begin{array}{cccc} \underbrace{\begin{matrix} 1 & \cdots & 1 \\ \vdots & & \vdots \\ 1 & \cdots & 1 \end{matrix}}_{a \text{ columns}} & \underbrace{\begin{matrix} 1 & \cdots & 1 \\ \vdots & & \vdots \\ 1 & \cdots & 1 \end{matrix}}_{b \text{ columns}} & \underbrace{\begin{matrix} 0 & \cdots & 0 \\ \vdots & & \vdots \\ 0 & \cdots & 0 \end{matrix}}_{c \text{ columns}} & \underbrace{\begin{matrix} 0 & \cdots & 0 \\ \vdots & & \vdots \\ 0 & \cdots & 0 \end{matrix}}_{d \text{ columns}} \end{array}\right]. \tag{5.15}$$

We now consider the four separate subcases that are dependent upon the Legendre symbols of the prime factors appended onto α.

Case I.1.A:
For the given pattern of Legendre symbols, the $(\delta + t) \times (\delta + t)$ **A** matrix described in Theorem 3.15 has the form

$$\mathbf{A_n} = \left[\begin{array}{c|ccccc} \mathbf{A}_\alpha & & & \mathbf{0} & & \\ \hline & a_{d+1} & 0 & \cdots & \cdots & 0 \\ & 1 & a_{d+2} & \ddots & & \vdots \\ \mathbf{T} & \vdots & \ddots & \ddots & \ddots & \vdots \\ & \vdots & & \ddots & a_{t-1} & 0 \\ & 1 & \cdots & \cdots & 1 & a_t \end{array}\right] = \left[\begin{array}{c|c} \mathbf{A}_\alpha & \mathbf{0} \\ \hline \mathbf{T} & \mathbf{A}^* \end{array}\right]. \tag{5.16}$$

Note that the entries along the diagonal in $\mathbf{A}^*$ vary according to the parity of the numbers $(c+d)$ and $(t-d)$. By knowing the parity of these quantities, we can determine whether there are an even or odd number of ones in each of the final $(t-d)$ rows in $\mathbf{A_n}$. This information, when combined with Equation (3.14), allows us to easily deduce the values of the diagonal elements in $\mathbf{A}^*$. These values are listed in Table 5.4.

Table 5.4: Diagonal entries in the matrix $\mathbf{A_n}$ in Case I.1.A of Theorem 5.5

Case	**Parity of** $(\boldsymbol{c+d})$	**Parity of** $(\boldsymbol{t-d})$	**Values of the Entries** $\boldsymbol{a_{d+1}, a_{d+2}, \ldots, a_{t-1}, a_t}$
1	Even	Odd	$0, 1, 0, 1, 0, \ldots, 1, 0$
2	Even	Even	$0, 1, 0, 1, \ldots, 0, 1$
3	Odd	Odd	$1, 0, 1, 0, 1, \ldots, 0, 1$
4	Odd	Even	$1, 0, 1, 0, \ldots, 1, 0$

We consider the first two cases listed in Table 5.4, and form the $(2\delta + 2t) \times (2\delta + 2t)$ Monsky matrix $\mathbf{M_o}$ for n by using Equation (3.16). It can be written as

$$\mathbf{M_o} = \left[\begin{array}{cc|cc} \mathbf{A}_\alpha + \mathbf{D}^\alpha_\mathbf{2} & \mathbf{0} & \mathbf{D}^\alpha_\mathbf{2} & \mathbf{0} \\ \hline \mathbf{T} & \mathbf{A}^* + \mathbf{I_{t-d}} & \mathbf{0} & \mathbf{I_{t-d}} \\ \hline\hline \mathbf{D}^\alpha_\mathbf{2} & \mathbf{0} & \mathbf{A}_\alpha + \mathbf{D}^\alpha_\mathbf{-2} & \mathbf{0} \\ \hline \mathbf{0} & \mathbf{I_{t-d}} & \mathbf{T} & \mathbf{A}^* \end{array}\right],$$

where $\mathbf{D}_\mathbf{2}^\alpha$, $\mathbf{D}_{-\mathbf{2}}^\alpha$, $\mathbf{T}$, and $\mathbf{A}^*$ are described in Equations (5.12), (5.13), (5.14), and (5.16), respectfully. By applying Equation (5.9) from Lemma 5.6, we can transform $\mathbf{M_o}$ into

$$\mathbf{M_o^*} = \left[\begin{array}{c|c||c|c} \mathbf{A}_\alpha + \mathbf{D}_\mathbf{2}^\alpha & \mathbf{D}_\mathbf{2}^\alpha & \mathbf{0} & \mathbf{0} \\ \hline \mathbf{D}_\mathbf{2}^\alpha & \mathbf{A}_\alpha + \mathbf{D}_{-\mathbf{2}}^\alpha & \mathbf{0} & \mathbf{0} \\ \hline\hline \mathbf{0} & \mathbf{T} & \mathbf{I_{t-d}} & \mathbf{A}^* \\ \hline \mathbf{T} & \mathbf{0} & \mathbf{A}^* + \mathbf{I_{t-d}} & \mathbf{I_{t-d}} \end{array}\right].$$

Note that by Lemma 5.6,

$$\det(\mathbf{M_o}) = \det(\mathbf{M_o^*}).$$

To compute the determinant of $\mathbf{M_o}$, and hence determine the rank of this matrix, we use Proposition 2.27. However, before doing this, we carry out $(t-d-1)$ row replacements in $\mathbf{M_o^*}$ to reduce the $\mathbf{A}^*$ block in $\mathbf{M_o^*}$ to the $(t-d)\times(t-d)$ zero matrix. Because the operations vary slightly for each of cases 1 and 2, we list them below using the notation defined in Section 2.3 and Equation (5.11).

Case 1:

$$\begin{array}{rcl} R_{2\delta+2d+2} & \longrightarrow & R_{2\delta+2d+2} + (R_{\omega+2} + R_{\omega+1}) \\ R_{2\delta+2d+3} & \longrightarrow & R_{2\delta+2d+3} + (R_{\omega+2} + R_{\omega+1}) \\ R_{2\delta+2d+4} & \longrightarrow & R_{2\delta+2d+4} + (R_{\omega+4} + R_{\omega+3} + R_{\omega+2} + R_{\omega+1}) \\ R_{2\delta+2d+5} & \longrightarrow & R_{2\delta+2d+5} + (R_{\omega+4} + R_{\omega+3} + R_{\omega+2} + R_{\omega+1}) \\ & \vdots & \\ R_{\omega-3} & \longrightarrow & R_{\omega-3} + (R_{2\delta+2t-3} + R_{2\delta+2t-4} + \cdots + R_{\omega+2} + R_{\omega+1}) \\ R_{\omega-2} & \longrightarrow & R_{\omega-2} + (R_{2\delta+2t-3} + R_{2\delta+2t-4} + \cdots + R_{\omega+2} + R_{\omega+1}) \\ R_{\omega-1} & \longrightarrow & R_{\omega-1} + (R_{2\delta+2t-1} + R_{2\delta+2t-2} + \cdots + R_{\omega+2} + R_{\omega+1}) \\ R_{\omega} & \longrightarrow & R_{\omega} + (R_{2\delta+2t-1} + R_{2\delta+2t-2} + \cdots + R_{\omega+2} + R_{\omega+1}) \end{array}$$

Case 2:

$$\begin{array}{rcl}
R_{2\delta+2d+2} & \longrightarrow & R_{2\delta+2d+2} + (R_{\omega+2} + R_{\omega+1}) \\
R_{2\delta+2d+3} & \longrightarrow & R_{2\delta+2d+3} + (R_{\omega+2} + R_{\omega+1}) \\
R_{2\delta+2d+4} & \longrightarrow & R_{2\delta+2d+4} + (R_{\omega+4} + R_{\omega+3} + R_{\omega+2} + R_{\omega+1}) \\
R_{2\delta+2d+5} & \longrightarrow & R_{2\delta+2d+5} + (R_{\omega+4} + R_{\omega+3} + R_{\omega+2} + R_{\omega+1}) \\
 & \vdots & \\
R_{\omega-4} & \longrightarrow & R_{\omega-4} + (R_{2\delta+2t-4} + R_{2\delta+2t-5} + \cdots + R_{\omega+2} + R_{\omega+1}) \\
R_{\omega-3} & \longrightarrow & R_{\omega-3} + (R_{2\delta+2t-4} + R_{2\delta+2t-5} + \cdots + R_{\omega+2} + R_{\omega+1}) \\
R_{\omega-2} & \longrightarrow & R_{\omega-2} + (R_{2\delta+2t-2} + R_{2\delta+2t-3} + \cdots + R_{\omega+2} + R_{\omega+1}) \\
R_{\omega-1} & \longrightarrow & R_{\omega-1} + (R_{2\delta+2t-2} + R_{2\delta+2t-3} + \cdots + R_{\omega+2} + R_{\omega+1}) \\
R_{\omega} & \longrightarrow & R_{\omega} + (R_{2\delta+2t} + R_{2\delta+2t-1} + \cdots + R_{\omega+2} + R_{\omega+1})
\end{array}$$

Since we are working over $\mathbb{F}_2$, the $\mathbf{A}^*$ matrix in $\mathbf{M}_\mathbf{o}^*$ is now reduced to the zero block, while all other entries in $\mathbf{M}_\mathbf{o}^*$ remain unchanged. For both case 1 and case 2, $\mathbf{M}_\mathbf{o}^*$ is transformed into

$$\mathbf{M}_\mathbf{o}^{**} = \left[\begin{array}{c|c||c|c}
\mathbf{A}_\alpha + \mathbf{D}_\mathbf{2}^\alpha & \mathbf{D}_\mathbf{2}^\alpha & \mathbf{0} & \mathbf{0} \\
\hline
\mathbf{D}_\mathbf{2}^\alpha & \mathbf{A}_\alpha + \mathbf{D}_{-\mathbf{2}}^\alpha & \mathbf{0} & \mathbf{0} \\
\hline\hline
\mathbf{0} & \mathbf{T} & \mathbf{I}_{\mathbf{t}-\mathbf{d}} & \mathbf{0}_{\mathbf{t}-\mathbf{d}} \\
\hline
\mathbf{T} & \mathbf{0} & \mathbf{A}^* + \mathbf{I}_{\mathbf{t}-\mathbf{d}} & \mathbf{I}_{\mathbf{t}-\mathbf{d}}
\end{array}\right].$$

Since

$$\left[\begin{array}{c|c}
\mathbf{I}_{\mathbf{t}-\mathbf{d}} & \mathbf{0}_{\mathbf{t}-\mathbf{d}} \\
\hline
\mathbf{A}^* + \mathbf{I}_{\mathbf{t}-\mathbf{d}} & \mathbf{I}_{\mathbf{t}-\mathbf{d}}
\end{array}\right]$$

is a lower triangular matrix with ones along its diagonal, its determinant is equal to one. Therefore, by applying Proposition 2.27 to $\mathbf{M}_\mathbf{o}^{**}$, we deduce that

$$\det(\mathbf{M}_\mathbf{o}) = \det(\mathbf{M}_\mathbf{o}^{**}) = \det\left[\begin{array}{c|c}
\mathbf{A}_\alpha + \mathbf{D}_\mathbf{2}^\alpha & \mathbf{D}_\mathbf{2}^\alpha \\
\hline
\mathbf{D}_\mathbf{2}^\alpha & \mathbf{A}_\alpha + \mathbf{D}_{-\mathbf{2}}^\alpha
\end{array}\right]. \tag{5.17}$$

Notice that the square matrix of order $(2\delta + 2d)$ within the determinant calculation above is precisely the Monsky matrix for α. Recall that by our original assumption, $s(\alpha) = 0$. As a result, Equation (3.15) implies that the Monsky matrix corresponding to α has full rank. It follows from Equation (5.17) that $\mathbf{M}_\mathbf{o}$ has full rank. Thus, when $(c + d)$ is even in Case I.1.A, $s(n) = 0$ and n is a non-congruent number.

We now consider cases 3 and 4 in Table 5.4. As in cases 1 and 2, we first construct the $(2\delta + 2t) \times (2\delta + 2t)$ Monsky matrix $\mathbf{M_o}$ for n. We then apply Equation (5.10) from Lemma 5.6 to transform $\mathbf{M_o}$ into

$$\mathbf{M'_o} = \left[\begin{array}{c|c||c|c} \mathbf{A}_\alpha + \mathbf{D}^{\alpha}_{\mathbf{2}} & \mathbf{D}^{\alpha}_{\mathbf{2}} & \mathbf{0} & \mathbf{0} \\ \hline \mathbf{D}^{\alpha}_{\mathbf{2}} & \mathbf{A}_\alpha + \mathbf{D}^{\alpha}_{\mathbf{-2}} & \mathbf{0} & \mathbf{0} \\ \hline\hline \mathbf{T} & \mathbf{0} & \mathbf{I_{t-d}} & \mathbf{A}^* + \mathbf{I_{t-d}} \\ \hline \mathbf{0} & \mathbf{T} & \mathbf{A}^* & \mathbf{I_{t-d}} \end{array}\right],$$

where the matrices $\mathbf{D}^{\alpha}_{\mathbf{2}}$, $\mathbf{D}^{\alpha}_{\mathbf{-2}}$, $\mathbf{T}$, and $\mathbf{A}^*$ are given by Equations (5.12), (5.13), (5.14), and (5.16), respectfully. Notice that the $\mathbf{A}^* + \mathbf{I_{t-d}}$ block in case 3 is identical to the $\mathbf{A}^*$ block in case 1. Therefore, the set of $(t - d - 1)$ row operations described in case 1 can also be applied in case 3 to transform $\mathbf{M'_o}$ into

$$\mathbf{M''_o} = \left[\begin{array}{c|c||c|c} \mathbf{A}_\alpha + \mathbf{D}^{\alpha}_{\mathbf{2}} & \mathbf{D}^{\alpha}_{\mathbf{2}} & \mathbf{0} & \mathbf{0} \\ \hline \mathbf{D}^{\alpha}_{\mathbf{2}} & \mathbf{A}_\alpha + \mathbf{D}^{\alpha}_{\mathbf{-2}} & \mathbf{0} & \mathbf{0} \\ \hline\hline \mathbf{T} & \mathbf{0} & \mathbf{I_{t-d}} & \mathbf{0_{t-d}} \\ \hline \mathbf{0} & \mathbf{T} & \mathbf{A}^* & \mathbf{I_{t-d}} \end{array}\right]. \tag{5.18}$$

Similarly, the $\mathbf{A}^* + \mathbf{I_{t-d}}$ block in case 4 is identical to the $\mathbf{A}^*$ block in case 2. This means that the matrix $\mathbf{M''_o}$, given by Equation (5.18), can be obtained by applying the same row replacement operations used in case 2. The remainder of the proof of cases 3 and 4 follows the process described in the proof of cases 1 and 2. We conclude that in Case I.1.A, $s(n) = 0$ and n is a non-congruent number.

Case I.1.B:
We split the proof of Case I.1.B into two subcases according to the parity of $(t - d)$, and start by considering the even case. The square $\mathbf{A}$ matrix of order $(\delta + t)$ corresponding to n has the form

$$\mathbf{A_n} = \left[\begin{array}{c|ccccccc}
\mathbf{A}_\alpha & \multicolumn{7}{c}{\mathbf{T}^T} \\ \hline
 & 1 & 1 & 1 & \cdots & \cdots & \cdots & 1 \\
 & 0 & 0 & 1 & & & & \vdots \\
 & 0 & 0 & 1 & \ddots & & & \vdots \\
\mathbf{0} & \vdots & & \ddots & \ddots & \ddots & & \vdots \\
 & \vdots & & & \ddots & 0 & 1 & 1 \\
 & \vdots & & & & 0 & 1 & 1 \\
 & 0 & \cdots & \cdots & \cdots & 0 & 0 & 0
\end{array}\right], \tag{5.19}$$

where $\mathbf{T}^T$ is the transpose of the matrix defined in Equation (5.14). Since we are working over $\mathbb{F}_2$ and $\mathbf{T}^T$ has dimension $(\delta+d)\times(t-d)$ with $(t-d)$ even, the elements along the diagonal in the upper left block of $\mathbf{A_n}$ are unaffected by the entries in $\mathbf{T}^T$. Also, notice that the block in the lower right corner of $\mathbf{A_n}$ is a $(t-d)\times(t-d)$ matrix with ones above its diagonal; this results in an alternating pattern of ones and zeros along the main diagonal of the block.

We construct the $(2\delta+2t)\times(2\delta+2t)$ Monsky matrix $\mathbf{M_o}$ for n by using Equation (3.16) and apply Equation (5.9) from Lemma 5.6 to transform it into

$$\mathbf{M_o^*} = \left[\begin{array}{c|c||ccccc|ccccc}
\mathbf{A}_\alpha + \mathbf{D}_\mathbf{2}^\alpha & \mathbf{D}_\mathbf{2}^\alpha & \multicolumn{5}{c|}{\mathbf{T}^T} & \multicolumn{5}{c}{\mathbf{0}} \\ \hline
\mathbf{D}_\mathbf{2}^\alpha & \mathbf{A}_\alpha + \mathbf{D}_\mathbf{-2}^\alpha & \multicolumn{5}{c|}{\mathbf{0}} & \multicolumn{5}{c}{\mathbf{T}^T} \\ \hline\hline
 & & & & & & & 1 & 1 & \cdots & \cdots & 1 \\
 & & & & & & & 0 & 0 & \ddots & & \vdots \\
\mathbf{0} & \mathbf{0} & \multicolumn{5}{c|}{\mathbf{I_{t-d}}} & \vdots & \ddots & \ddots & \ddots & \vdots \\
 & & & & & & & \vdots & & \ddots & 1 & 1 \\
 & & & & & & & 0 & \cdots & \cdots & 0 & 0 \\ \hline
 & & 0 & 1 & \cdots & \cdots & 1 & & & & & \\
 & & 0 & 1 & \ddots & & \vdots & & & & & \\
\mathbf{0} & \mathbf{0} & \vdots & \ddots & \ddots & \ddots & \vdots & \multicolumn{5}{c}{\mathbf{I_{t-d}}} \\
 & & \vdots & & \ddots & 0 & 1 & & & & & \\
 & & 0 & \cdots & \cdots & 0 & 1 & & & & &
\end{array}\right],$$

where $\mathbf{D}_\mathbf{2}^\alpha$ and $\mathbf{D}_{-\mathbf{2}}^\alpha$ are described in Equations (5.12) and (5.13), respectively. Next, we carry out the following $(t-d-1)$ row operations to reduce $\mathbf{M}_\mathbf{o}^*$ so that its determinant can be easily calculated using Proposition 2.27.

$$\begin{array}{rcl}
R_{2\delta+2d+1} & \longrightarrow & R_{2\delta+2d+1} + (R_{2\delta+2t} + R_{2\delta+2t-1} + \cdots + R_{\omega+2} + R_{\omega+1}) \\
R_{2\delta+2d+2} & \longrightarrow & R_{2\delta+2d+2} + (R_{2\delta+2t} + R_{2\delta+2t-1} + \cdots + R_{\omega+4} + R_{\omega+3}) \\
R_{2\delta+2d+3} & \longrightarrow & R_{2\delta+2d+3} + (R_{2\delta+2t} + R_{2\delta+2t-1} + \cdots + R_{\omega+4} + R_{\omega+3}) \\
R_{2\delta+2d+4} & \longrightarrow & R_{2\delta+2d+4} + (R_{2\delta+2t} + R_{2\delta+2t-1} + \cdots + R_{\omega+6} + R_{\omega+5}) \\
 & \vdots & \\
R_{\omega-4} & \longrightarrow & R_{\omega-4} + (R_{2\delta+2t} + R_{2\delta+2t-1} + R_{2\delta+2t-2} + R_{2\delta+2t-3}) \\
R_{\omega-3} & \longrightarrow & R_{\omega-3} + (R_{2\delta+2t} + R_{2\delta+2t-1} + R_{2\delta+2t-2} + R_{2\delta+2t-3}) \\
R_{\omega-2} & \longrightarrow & R_{\omega-2} + (R_{2\delta+2t} + R_{2\delta+2t-1}) \\
R_{\omega-1} & \longrightarrow & R_{\omega-1} + (R_{2\delta+2t} + R_{2\delta+2t-1})
\end{array}$$

These row operations transform the matrix $\mathbf{M}_\mathbf{o}^*$ into

$$\mathbf{M}_\mathbf{o}^{**} = \left[\begin{array}{c|c|ccccc|c}
\mathbf{A}_\alpha + \mathbf{D}_\mathbf{2}^\alpha & \mathbf{D}_\mathbf{2}^\alpha & \multicolumn{5}{c|}{\mathbf{T}^T} & \mathbf{0} \\
\hline
\mathbf{D}_\mathbf{2}^\alpha & \mathbf{A}_\alpha + \mathbf{D}_{-\mathbf{2}}^\alpha & \multicolumn{5}{c|}{\mathbf{0}} & \mathbf{T}^T \\
\hline\hline
\mathbf{0} & \mathbf{0} & \multicolumn{5}{c|}{\mathbf{I_{t-d}}} & \mathbf{0_{t-d}} \\
\hline
 & & 0 & 1 & \cdots & \cdots & 1 & \\
 & & 0 & 1 & \ddots & & \vdots & \\
\mathbf{0} & \mathbf{0} & \vdots & \ddots & \ddots & \ddots & \vdots & \mathbf{I_{t-d}} \\
 & & \vdots & & \ddots & 0 & 1 & \\
 & & 0 & \cdots & \cdots & 0 & 1 &
\end{array}\right],$$

with

$$\det(\mathbf{M_o}) = \det(\mathbf{M}_\mathbf{o}^{**}).$$

The $(2t-2d) \times (2t-2d)$ block in the bottom right corner of $\mathbf{M}_\mathbf{o}^{**}$ is a lower triangular matrix with determinant equal to one, so Proposition 2.27 implies that

$$\det(\mathbf{M_o}) = \det \left[\begin{array}{c|c}
\mathbf{A}_\alpha + \mathbf{D}_\mathbf{2}^\alpha & \mathbf{D}_\mathbf{2}^\alpha \\
\hline
\mathbf{D}_\mathbf{2}^\alpha & \mathbf{A}_\alpha + \mathbf{D}_{-\mathbf{2}}^\alpha
\end{array}\right],$$

which is identical to Equation (5.17). Therefore, as in Case I.1.A, we conclude that $s(n) = 0$ and n is a non-congruent number when $(t-d)$ is even.

Finally, we consider the case where $(t-d)$ is odd, and form the $\mathbf{A}$ matrix for n,

$$\mathbf{A_n} = \left[\begin{array}{c|cccccc} \mathbf{A}_\alpha + \mathbf{J} & \multicolumn{6}{c}{\mathbf{T}^T} \\ \cline{2-7} & 0 & 1 & 1 & \cdots & \cdots & 1 \\ & 0 & 1 & 1 & & & \vdots \\ \mathbf{0} & 0 & 0 & 0 & \ddots & & \vdots \\ & \vdots & & \ddots & \ddots & \ddots & \vdots \\ & \vdots & & & \ddots & 1 & 1 \\ & 0 & \cdots & \cdots & \cdots & 0 & 0 \end{array}\right],$$

where

$$\mathbf{J} = \left[\begin{array}{c|c} \mathbf{0_{a+b}} & \mathbf{0} \\ \hline \mathbf{0} & \mathbf{I_{c+d}} \end{array}\right]. \tag{5.20}$$

The matrix $\mathbf{J}$ is introduced to account for the fact that when $(t-d)$ is odd, the $(c+d)$ rows of ones in $\mathbf{T}^T$ affect the diagonal entries in the upper left block of $\mathbf{A_n}$. Also, notice that the elements along the main diagonal in the lower right block of $\mathbf{A_n}$ alternate between zeros and ones, but that the pattern is different from the one in the matrix described by Equation (5.19).

We form the Monsky matrix $\mathbf{M_o}$ corresponding to n and follow the series of steps outlined in the proof of the case where $(t-d)$ is even. That is, we perform a set of row operations and apply Proposition 2.27 to deduce that

$$\det(\mathbf{M_o}) = \det \left[\begin{array}{c|c} \mathbf{A}_\alpha + \mathbf{J} + \mathbf{D}^\alpha_\mathbf{2} & \mathbf{D}^\alpha_\mathbf{2} \\ \hline \mathbf{D}^\alpha_\mathbf{2} & \mathbf{A}_\alpha + \mathbf{J} + \mathbf{D}^\alpha_\mathbf{-2} \end{array}\right]. \tag{5.21}$$

Since we are working over $\mathbb{F}_2$,

$$\mathbf{D}^\alpha_\mathbf{2} = \mathbf{D}^\alpha_\mathbf{-2} + \mathbf{J} \qquad \text{and} \qquad \mathbf{D}^\alpha_\mathbf{-2} = \mathbf{D}^\alpha_\mathbf{2} + \mathbf{J},$$

where the matrices $\mathbf{D}^\alpha_\mathbf{2}$, $\mathbf{D}^\alpha_\mathbf{-2}$, and $\mathbf{J}$ are given by Equations (5.12), (5.13), and (5.20), respectfully. Therefore, Equation (5.21) becomes

$$\det(\mathbf{M_o}) = \det \left[\begin{array}{c|c} \mathbf{A}_\alpha + \mathbf{D}^\alpha_\mathbf{-2} & \mathbf{D}^\alpha_\mathbf{2} \\ \hline \mathbf{D}^\alpha_\mathbf{2} & \mathbf{A}_\alpha + \mathbf{D}^\alpha_\mathbf{2} \end{array}\right].$$

This can be rewritten in the form of Equation (5.17) by applying elementary row and column operations to the block matrix. As before, we conclude that $s(n) = 0$ and n is a non-congruent number when $(t-d)$ is odd.

Case I.1.C:
The square **A** matrix of order $(\delta + t)$ corresponding to n is

$$\mathbf{A_n} = \left[\begin{array}{c|ccccc}
 & 1 & \cdots & \cdots & \cdots & 1 \\
\mathbf{A}_\alpha & \vdots & & & & \vdots \\
 & 1 & \cdots & \cdots & \cdots & 1 \\
\hline
 & a_{d+1} & 1 & \cdots & \cdots & 1 \\
 & 0 & a_{d+2} & \ddots & & \vdots \\
\mathbf{U} & \vdots & \ddots & \ddots & \ddots & \vdots \\
 & \vdots & & \ddots & a_{t-1} & 1 \\
 & 0 & \cdots & \cdots & 0 & a_t
\end{array}\right],$$

where **U** is given by Equation (5.15). Because we are working over $\mathbb{F}_2$ and the upper right block of $\mathbf{A_n}$ has an even number ones in each of its rows, the elements along the diagonal in the upper left block of $\mathbf{A_n}$ remain the same as those in $\mathbf{A}_\alpha$. However, the diagonal entries in the lower right block in $\mathbf{A_n}$ vary according to the parity of $(a+b)$. Since $(t-d)$ is even, the block in the lower right corner of $\mathbf{A_n}$ has an even number of columns, and hence

$$(a_{d+1}, a_{d+2}, \ldots, a_{t-1}, a_t) = \begin{cases} (1, 0, \ldots, 1, 0) & \text{if } (a+b) \text{ is even,} \\ (0, 1, \ldots, 0, 1) & \text{if } (a+b) \text{ is odd.} \end{cases}$$

We construct the Monsky matrix $\mathbf{M_o}$ for n by using Equation (3.16). When $(a+b)$ is even, we apply Equation (5.9) from Lemma 5.6 to $\mathbf{M_o}$, so that it becomes

$$\mathbf{M}^*_{\mathbf{o}} = \left[\begin{array}{c|c|c|c}
\mathbf{A}_\alpha + \mathbf{D}^{\alpha}_{\mathbf{2}} & \mathbf{D}^{\alpha}_{\mathbf{2}} & \begin{matrix} 1 & \cdots & \cdots & \cdots & 1 \\ \vdots & & & & \vdots \\ 1 & \cdots & \cdots & \cdots & 1 \end{matrix} & \mathbf{0} \\
\hline
\mathbf{D}^{\alpha}_{\mathbf{2}} & \mathbf{A}_\alpha + \mathbf{D}^{\alpha}_{\mathbf{-2}} & \mathbf{0} & \begin{matrix} 1 & \cdots & \cdots & \cdots & 1 \\ \vdots & & & & \vdots \\ 1 & \cdots & \cdots & \cdots & 1 \end{matrix} \\
\hline\hline
\mathbf{0} & \mathbf{U} & \mathbf{I}_{\mathbf{t-d}} & \begin{matrix} 1 & 1 & \cdots & \cdots & 1 \\ 0 & 0 & \ddots & & \vdots \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ \vdots & & \ddots & 1 & 1 \\ 0 & \cdots & \cdots & 0 & 0 \end{matrix} \\
\hline
\mathbf{U} & \mathbf{0} & \begin{matrix} 0 & 1 & \cdots & \cdots & 1 \\ 0 & 1 & \ddots & & \vdots \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ \vdots & & \ddots & 0 & 1 \\ 0 & \cdots & \cdots & 0 & 1 \end{matrix} & \mathbf{I}_{\mathbf{t-d}}
\end{array}\right].$$

We modify this matrix by implementing a series of row operations. We add all of the final $(t-d)$ rows in $\mathbf{M}^*_{\mathbf{o}}$ to each of rows $(\delta+d+1)$ through $(2\delta+2d)$ in $\mathbf{M}^*_{\mathbf{o}}$. These elementary operations transform the rightmost block of ones in $\mathbf{M}^*_{\mathbf{o}}$ into a zero block while leaving the remaining entries in $\mathbf{M}^*_{\mathbf{o}}$ unchanged. We reduce the nonzero block immediately above the identity matrix in the lower right corner of $\mathbf{M}^*_{\mathbf{o}}$ to the zero matrix by carrying out the $(t-d-1)$ row replacements listed in Case I.1.B. Finally, we add each of rows $(2\delta+2d+1)$ through $(2\delta+t+d)$ to the first $(\delta+d)$ rows in $\mathbf{M}^*_{\mathbf{o}}$.

Altogether, these operations transform $\mathbf{M_o^*}$ into

$$\mathbf{M_o^{**}} = \left[\begin{array}{c|c||c|c}
\mathbf{A}_\alpha + \mathbf{D_2^\alpha} & \mathbf{D_2^\alpha} & \mathbf{0} & \mathbf{0} \\
\hline
\mathbf{D_2^\alpha} & \mathbf{A}_\alpha + \mathbf{D_{-2}^\alpha} & \mathbf{0} & \mathbf{0} \\
\hline\hline
\mathbf{0} & \mathbf{U} & \mathbf{I_{t-d}} & \mathbf{0_{t-d}} \\
\hline
\mathbf{U} & \mathbf{0} & \begin{matrix} 0 & 1 & \cdots & \cdots & 1 \\ 0 & 1 & \ddots & & \vdots \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ \vdots & & \ddots & 0 & 1 \\ 0 & \cdots & \cdots & 0 & 1 \end{matrix} & \mathbf{I_{t-d}}
\end{array}\right].$$

We apply Proposition 2.27 to $\mathbf{M_o^{**}}$ to obtain Equation (5.17). As before, it follows that $s(n) = 0$ and n is a non-congruent number when $(a+b)$ is even.

Finally, we consider the case where $(a + b)$ is odd, and use Equation (5.10) from Lemma 5.6 to transform $\mathbf{M_o}$ into

$$\mathbf{M_o'} = \left[\begin{array}{c|c||c|c}
\mathbf{A}_\alpha + \mathbf{D_2^\alpha} & \mathbf{D_2^\alpha} & \mathbf{0} & \begin{matrix} 1 & \cdots & \cdots & \cdots & 1 \\ \vdots & & & & \vdots \\ 1 & \cdots & \cdots & \cdots & 1 \end{matrix} \\
\hline
\mathbf{D_2^\alpha} & \mathbf{A}_\alpha + \mathbf{D_{-2}^\alpha} & \begin{matrix} 1 & \cdots & \cdots & \cdots & 1 \\ \vdots & & & & \vdots \\ 1 & \cdots & \cdots & \cdots & 1 \end{matrix} & \mathbf{0} \\
\hline\hline
\mathbf{U} & \mathbf{0} & \mathbf{I_{t-d}} & \begin{matrix} 1 & 1 & \cdots & \cdots & 1 \\ 0 & 0 & \ddots & & \vdots \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ \vdots & & \ddots & 1 & 1 \\ 0 & \cdots & \cdots & 0 & 0 \end{matrix} \\
\hline
\mathbf{0} & \mathbf{U} & \begin{matrix} 0 & 1 & \cdots & \cdots & 1 \\ 0 & 1 & \ddots & & \vdots \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ \vdots & & \ddots & 0 & 1 \\ 0 & \cdots & \cdots & 0 & 1 \end{matrix} & \mathbf{I_{t-d}}
\end{array}\right].$$

Notice that this matrix is very similar to the matrix $\mathbf{M_o^*}$ in the case where $(a + b)$ is even; of specific interest is the fact that the lower right square blocks of order $(2t - 2d)$ in each matrix are identical. Therefore, the case where $(a + b)$ is odd can be proved analogously to the case where $(a + b)$ is even. Thus, we conclude that $s(n) = 0$ and n is a non-congruent number irrespective of the parity of $(a + b)$.

Case I.1.D:
We construct the $(\delta + t) \times (\delta + t)$ $\mathbf{A}$ matrix for n from the Legendre symbol conditions imposed on the tail of primes appended onto α. This matrix has the form

$$\mathbf{A_n} = \left[\begin{array}{ccc|ccccc}
\multicolumn{3}{c|}{\mathbf{A}_\alpha} & \multicolumn{5}{c}{\mathbf{U}^T} \\ \hline
1 & \cdots & 1 & a_{d+1} & 0 & \cdots & \cdots & 0 \\
\vdots & & \vdots & 1 & a_{d+2} & \ddots & & \vdots \\
\vdots & & \vdots & \vdots & \ddots & \ddots & \ddots & \vdots \\
\vdots & & \vdots & \vdots & & \ddots & a_{t-1} & 0 \\
1 & \cdots & 1 & 1 & \cdots & \cdots & 1 & a_t
\end{array}\right],$$

where $\mathbf{U}^T$ is the transpose of the matrix in Equation (5.15). Since the $(t-d)$ elements in each row of $\mathbf{U}^T$ are either all zeroes or all ones, the diagonal entries in the upper left block of $\mathbf{A_n}$ are not affected by the elements in $\mathbf{U}^T$, and hence remain the same as those in $\mathbf{A}_\alpha$. However, the entries along the diagonal in the lower right block in $\mathbf{A_n}$ depend upon the parity of the quantity $(\delta + d)$. By assumption $(t - d)$ is even, so we can deduce that

$$(a_{d+1}, a_{d+2}, \ldots, a_{t-1}, a_t) = \begin{cases} (0, 1, \ldots, 0, 1) & \text{if } (\delta + d) \text{ is even,} \\ (1, 0, \ldots, 1, 0) & \text{if } (\delta + d) \text{ is odd.} \end{cases}$$

We consider the case where $(\delta + d)$ is even and form the Monsky matrix $\mathbf{M_o}$ for n. We apply Equation (5.9) from Lemma 5.6 to rearrange the blocks in $\mathbf{M_o}$ and transform it into

$$\mathbf{M_o^*} = \left[\begin{array}{c|c||c|c}
\mathbf{A}_\alpha + \mathbf{D_2^\alpha} & \mathbf{D_2} & \mathbf{U}^T & \mathbf{0} \\ \hline
\mathbf{D_2^\alpha} & \mathbf{A}_\alpha + \mathbf{D_{-2}^\alpha} & \mathbf{0} & \mathbf{U}^T \\ \hline \hline
\mathbf{0} & \begin{matrix} 1 & \cdots & 1 \\ \vdots & & \vdots \\ \vdots & & \vdots \\ \vdots & & \vdots \\ 1 & \cdots & 1 \end{matrix} & \mathbf{I_{t-d}} & \begin{matrix} 0 & 0 & \cdots & \cdots & 0 \\ 1 & 1 & \ddots & & \vdots \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ \vdots & & \ddots & 0 & 0 \\ 1 & \cdots & \cdots & 1 & 1 \end{matrix} \\ \hline
\begin{matrix} 1 & \cdots & 1 \\ \vdots & & \vdots \\ \vdots & & \vdots \\ \vdots & & \vdots \\ 1 & \cdots & 1 \end{matrix} & \mathbf{0} & \begin{matrix} 1 & 0 & \cdots & \cdots & 0 \\ 1 & 0 & \ddots & & \vdots \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ \vdots & & \ddots & 1 & 0 \\ 1 & \cdots & \cdots & 1 & 0 \end{matrix} & \mathbf{I_{t-d}}
\end{array}\right].$$

To apply Proposition 2.27 to this matrix, we must reduce the two $\mathbf{U}^T$ blocks in the upper right corner of $\mathbf{M_o^*}$ to zero blocks by carrying out row operations. Specifically, we add the final $(t-d)$ rows in $\mathbf{M_o^*}$ to each of rows $(\delta + d + 1)$ through $(\delta + d + a + b)$. Notice that these $(a+b)$ row replacements only affect the elements in the rightmost $\mathbf{U}^T$ block of $\mathbf{M_o^*}$, leaving the remaining entries in $\mathbf{M_o^*}$ unchanged. We then carry out the same set of $(t-d-1)$ row replacements as in case 2 of Case 1.I.A to reduce the $(2t-2d) \times (2t-2d)$ block in the bottom right corner of $\mathbf{M_o^*}$ to a lower triangular matrix. Finally, we add all of rows $(2\delta+2d+1)$ through $(2\delta+t+d)$ to each of the first $(a+b)$ rows in $\mathbf{M_o^*}$. This set of row operations transforms $\mathbf{M_o^*}$ into

$$\mathbf{M_o^{**}} = \left[\begin{array}{c|c||c|c} \mathbf{A}_\alpha + \mathbf{D}_\mathbf{2}^\alpha & \mathbf{D_2} & \mathbf{0} & \mathbf{0} \\ \hline \mathbf{D}_\mathbf{2}^\alpha & \mathbf{A}_\alpha + \mathbf{D}_{-\mathbf{2}}^\alpha & \mathbf{0} & \mathbf{0} \\ \hline\hline \mathbf{0} & \begin{array}{ccc} 1 & \cdots & 1 \\ \vdots & & \vdots \\ 1 & \cdots & 1 \end{array} & \mathbf{I_{t-d}} & \mathbf{0_{t-d}} \\ \hline \begin{array}{ccc} 1 & \cdots & 1 \\ \vdots & & \vdots \\ \vdots & & \vdots \\ \vdots & & \vdots \\ 1 & \cdots & 1 \end{array} & \mathbf{0} & \begin{array}{ccccc} 1 & 0 & \cdots & \cdots & 0 \\ 1 & 0 & \ddots & & \vdots \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ \vdots & & \ddots & 1 & 0 \\ 1 & \cdots & \cdots & 1 & 0 \end{array} & \mathbf{I_{t-d}} \end{array}\right].$$

Since

$$\det(\mathbf{M_o}) = \det(\mathbf{M_o^{**}}),$$

Proposition 2.27 yields

$$\det(\mathbf{M_o}) = \det \left[\begin{array}{c|c} \mathbf{A}_\alpha + \mathbf{D}_\mathbf{2}^\alpha & \mathbf{D}_\mathbf{2}^\alpha \\ \hline \mathbf{D}_\mathbf{2}^\alpha & \mathbf{A}_\alpha + \mathbf{D}_{-\mathbf{2}}^\alpha \end{array}\right].$$

This is identical to Equation (5.17). It follows that $s(n) = 0$ and n is non-congruent when $(\delta + d)$ is even.

In the case where $(\delta + d)$ is odd, we construct the Monsky matrix $\mathbf{M_o}$

for n and use Equation (5.10) from Lemma 5.6 to transform $\mathbf{M_o}$ into

$$\mathbf{M_o'} = \left[\begin{array}{c|c||c|c}
\mathbf{A}_\alpha + \mathbf{D_2^\alpha} & \mathbf{D_2} & \mathbf{0} & \mathbf{U}^T \\ \hline
\mathbf{D_2^\alpha} & \mathbf{A}_\alpha + \mathbf{D_{-2}^\alpha} & \mathbf{U}^T & \mathbf{0} \\ \hline\hline
\begin{matrix} 1 & \cdots & 1 \\ \vdots & & \vdots \\ \vdots & & \vdots \\ \vdots & & \vdots \\ 1 & \cdots & 1 \end{matrix} & \mathbf{0} & \mathbf{I_{t-d}} & \begin{matrix} 0 & 0 & \cdots & \cdots & 0 \\ 1 & 1 & \ddots & & \vdots \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ \vdots & & \ddots & 0 & 0 \\ 1 & \cdots & \cdots & 1 & 1 \end{matrix} \\ \hline
\mathbf{0} & \begin{matrix} 1 & \cdots & 1 \\ \vdots & & \vdots \\ \vdots & & \vdots \\ \vdots & & \vdots \\ 1 & \cdots & 1 \end{matrix} & \begin{matrix} 1 & 0 & \cdots & \cdots & 0 \\ 1 & 0 & \ddots & & \vdots \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ \vdots & & \ddots & 1 & 0 \\ 1 & \cdots & \cdots & 1 & 0 \end{matrix} & \mathbf{I_{t-d}}
\end{array}\right].$$

Because the matrices $\mathbf{M_o^*}$ for $(\delta + d)$ even and $\mathbf{M_o'}$ for $(\delta + d)$ odd are similar, we can follow the same process to prove the case where $(\delta + d)$ is odd. We conclude that, regardless of the parity of $(\delta + d)$, $s(n) = 0$ and n is a non-congruent number. □

Next, we prove that Case II.2.

Case II.2 Proof. We construct the $(\delta + t) \times (\delta + t)$ $\mathbf{D_2}$ and $\mathbf{D_{-2}}$ matrices for $n = \alpha s_{d+1} s_{d+2} \cdots s_t$,

$$\mathbf{D_2^n} = \left[\begin{array}{c|c} \mathbf{D_2^\alpha} & \mathbf{0} \\ \hline \mathbf{0} & \mathbf{I_{t-d}} \end{array}\right] \qquad \text{and} \qquad \mathbf{D_{-2}^n} = \left[\begin{array}{c|c} \mathbf{D_{-2}^\alpha} & \mathbf{0} \\ \hline \mathbf{0} & \mathbf{I_{t-d}} \end{array}\right],$$

where $\mathbf{D_2^\alpha}$ and $\mathbf{D_{-2}^\alpha}$ are the $(\delta+d) \times (\delta+d)$ diagonal matrices corresponding to α. We also define the $(\delta+d) \times (t-d)$ matrix $\mathbf{B}$ with the elements in each of its rows being either all equal to one or all equal to zero. In addition, we require that $\mathbf{B}$ contains an odd number of rows with entries all equal to one.

The Monsky matrix $\mathbf{M_o}$ for n can be written as

$$\begin{aligned}\mathbf{M_o} &= \left[\begin{array}{c|c} \mathbf{A_n}+\mathbf{D_2^n} & \mathbf{D_2^n} \\ \hline \mathbf{D_2^n} & \mathbf{A_n}+\mathbf{D^n_{-2}} \end{array}\right] \\ &= \left[\begin{array}{c|c||c|c} \mathbf{A}_\alpha+\mathbf{D}_\mathbf{2}^\alpha & \mathbf{B} & \mathbf{D}_\mathbf{2}^\alpha & \mathbf{0} \\ \hline \mathbf{B}^T & \mathbf{0_{t-d}} & \mathbf{0} & \mathbf{I_{t-d}} \\ \hline\hline \mathbf{D}_\mathbf{2}^\alpha & \mathbf{0} & \mathbf{A}_\alpha+\mathbf{D}^\alpha_{\mathbf{-2}} & \mathbf{B} \\ \hline \mathbf{0} & \mathbf{I_{t-d}} & \mathbf{B}^T & \mathbf{0_{t-d}} \end{array}\right].\end{aligned}$$

Notice that since $(t-d)$ is even, the sum of the elements in an arbitrary row of $\mathbf{B}$ is congruent to zero modulo two. Because we are working over $\mathbb{F}_2$, the elements along the main diagonal of the upper left blocks of $\mathbf{A_n}+\mathbf{D_2^n}$ and $\mathbf{A_n}+\mathbf{D^n_{-2}}$ in $\mathbf{M_o}$ are not affected by the entries in $\mathbf{B}$. Furthermore, seeing that there are an odd number of rows in $\mathbf{B}$ with elements all equal to one, there are an odd number of entries in each row of $\mathbf{B}^T$ that are equal to one. This allows us to determine that the diagonal elements in the lower right blocks of $\mathbf{A_n}+\mathbf{D_2^n}$ and $\mathbf{A_n}+\mathbf{D^n_{-2}}$ are all zero.

We apply Equation (5.9) from Lemma 5.6 to rearrange the blocks in $\mathbf{M_o}$ and transform it into

$$\mathbf{M_o^*} = \left[\begin{array}{c|c||c|c} \mathbf{A}_\alpha+\mathbf{D}_\mathbf{2}^\alpha & \mathbf{D}_\mathbf{2}^\alpha & \mathbf{B} & \mathbf{0} \\ \hline \mathbf{D}_\mathbf{2}^\alpha & \mathbf{A}_\alpha+\mathbf{D}^\alpha_{\mathbf{-2}} & \mathbf{0} & \mathbf{B} \\ \hline\hline \mathbf{0} & \mathbf{B}^T & \mathbf{I_{t-d}} & \mathbf{0_{t-d}} \\ \hline \mathbf{B}^T & \mathbf{0} & \mathbf{0_{t-d}} & \mathbf{I_{t-d}} \end{array}\right]. \tag{5.22}$$

Our goal is to reduce the two $\mathbf{B}$ blocks in $\mathbf{M_o^*}$ to zero matrices by carrying out a set of row operations. We begin by adding rows $(2\delta+2d+1)$ through $(2\delta+d+t)$ in $\mathbf{M_o^*}$ to each of the first $(\delta+d)$ rows in $\mathbf{M_o^*}$ that correspond to rows in $\mathbf{B}$ containing all ones. Notice that when we apply these row operations, the entries in $\mathbf{B}^T$ do not affect those in the $\mathbf{D}_\mathbf{2}^\alpha$ block. This is because each column in $\mathbf{B}^T$ contains elements that are either all ones or all zeros, and we are adding all of the $(t-d)$ rows of $\mathbf{B}^T$, where $(t-d)$ is even, to a given row in $\mathbf{D}_\mathbf{2}^\alpha$. An analogous procedure can be applied to transform the remaining $\mathbf{B}$ block in $\mathbf{M_o^*}$ into the zero matrix; this reduces $\mathbf{M_o^*}$ to

$$\mathbf{M_o^{**}} = \left[\begin{array}{c|c||c|c} \mathbf{A}_\alpha + \mathbf{D}_\mathbf{2}^\alpha & \mathbf{D}_\mathbf{2}^\alpha & \mathbf{0} & \mathbf{0} \\ \hline \mathbf{D}_\mathbf{2}^\alpha & \mathbf{A}_\alpha + \mathbf{D}_{-\mathbf{2}}^\alpha & \mathbf{0} & \mathbf{0} \\ \hline\hline \mathbf{0} & \mathbf{B}^T & \mathbf{I_{t-d}} & \mathbf{0_{t-d}} \\ \hline \mathbf{B}^T & \mathbf{0} & \mathbf{0_{t-d}} & \mathbf{I_{t-d}} \end{array}\right]. \tag{5.23}$$

Since we are working over $\mathbb{F}_2$, the elementary row and column operations that we applied to transform $\mathbf{M_o}$ into $\mathbf{M_o^{**}}$ do not affect the value of the determinant, so

$$\det(\mathbf{M_o}) = \det(\mathbf{M_o^{**}}).$$

Furthermore, by applying Proposition 2.27 to $\mathbf{M_o^{**}}$, we can deduce that

$$\det(\mathbf{M_o}) = \det \left[\begin{array}{c|c} \mathbf{A}_\alpha + \mathbf{D}_\mathbf{2}^\alpha & \mathbf{D}_\mathbf{2}^\alpha \\ \hline \mathbf{D}_\mathbf{2}^\alpha & \mathbf{A}_\alpha + \mathbf{D}_{-\mathbf{2}}^\alpha \end{array}\right]. \tag{5.24}$$

The block matrix in the determinant calculation immediately above is the Monsky matrix for α. Our original assumption that $s(\alpha) = 0$ implies that the Monsky matrix corresponding to α has full rank. Thus, by Equation (5.24), we conclude that $\mathbf{M_o}$ also has full rank, so $s(n) = 0$ and n is a non-congruent number. □

We now provide a proof of Case III.2.

Case III.2 Proof. We define $\mathbf{D}_\mathbf{2}^\alpha$ and $\mathbf{D}_{-\mathbf{2}}^\alpha$ to be the $(\delta+d)\times(\delta+d)$ diagonal $\mathbf{D_2}$ and $\mathbf{D_{-2}}$ matrices for α. The diagonal matrices corresponding to $n = \alpha s_{d+1}s_{d+2}\cdots s_t$ have the form

$$\mathbf{D_2^n} = \left[\begin{array}{c|c} \mathbf{D}_\mathbf{2}^\alpha & \mathbf{0} \\ \hline \mathbf{0} & \mathbf{0_{t-d}} \end{array}\right] \qquad \text{and} \qquad \mathbf{D_{-2}^n} = \left[\begin{array}{c|c} \mathbf{D}_{-\mathbf{2}}^\alpha & \mathbf{0} \\ \hline \mathbf{0} & \mathbf{0_{t-d}} \end{array}\right].$$

We write the $(2\delta+2t)\times(2\delta+2t)$ Monsky matrix for n as

$$\mathbf{M_o} = \left[\begin{array}{c|c||c|c} \mathbf{A}_\alpha + \mathbf{D}_\mathbf{2}^\alpha & \mathbf{B} & \mathbf{D}_\mathbf{2}^\alpha & \mathbf{0} \\ \hline \mathbf{B}^T & \mathbf{I_{t-d}} & \mathbf{0} & \mathbf{0_{t-d}} \\ \hline\hline \mathbf{D}_\mathbf{2}^\alpha & \mathbf{0} & \mathbf{A}_\alpha + \mathbf{D}_{-\mathbf{2}}^\alpha & \mathbf{B} \\ \hline \mathbf{0} & \mathbf{0_{t-d}} & \mathbf{B}^T & \mathbf{I_{t-d}} \end{array}\right],$$

where the block $\mathbf{B}$ is identical to that described in Case II.2.

As in Case II.2, we transform the two $\mathbf{B}$ blocks in $\mathbf{M_o}$ into zero blocks by carrying out row operations. Specifically, we add rows $(\delta+d+1)$ through $(\delta+t)$ in $\mathbf{M_o}$ to each of the first $(\delta+d)$ rows in $\mathbf{M_o}$ that correspond to rows in $\mathbf{B}$ containing all ones. This reduces the $\mathbf{B}$ block in the upper left quadrant of $\mathbf{M_o}$ to a zero block, while leaving the remaining entries in $\mathbf{M_o}$ unchanged. In addition, we add each of rows $(2\delta+d+t+1)$ through $(2\delta+2t)$ to any of rows $(\delta+t+1)$ through $(2\delta+t+d)$ in $\mathbf{M_o}$ that correspond to rows in $\mathbf{B}$ containing all ones. The matrix that results from applying this set of row operations to $\mathbf{M_o}$ is

$$\mathbf{M_o^*} = \left[\begin{array}{c|c|c|c} \mathbf{A}_\alpha + \mathbf{D}^\alpha_\mathbf{2} & \mathbf{0} & \mathbf{D}^\alpha_\mathbf{2} & \mathbf{0} \\ \cline{1-4} \mathbf{B}^T & \mathbf{I_{t-d}} & \mathbf{0} & \mathbf{0_{t-d}} \\ \hline\hline \mathbf{D}^\alpha_\mathbf{2} & \mathbf{0} & \mathbf{A}_\alpha + \mathbf{D}^\alpha_\mathbf{-2} & \mathbf{0} \\ \cline{1-4} \mathbf{0} & \mathbf{0_{t-d}} & \mathbf{B}^T & \mathbf{I_{t-d}} \end{array}\right].$$

By interchanging rows and columns in $\mathbf{M_o^*}$, it can be transformed into the matrix given by Equation (5.23) in Case II.2. Therefore, the remainder of the proof follows as in Case II.2, and we conclude that in Case III.2, $s(n) = 0$ and n is a non-congruent number. □

Finally, we complete the proof of Theorem 5.5 by verifying that Case III.3 generates non-congruent numbers. Note that Case III.3 of Theorem 5.5 provides a generalization of Theorem 5.1.

Case III.3 Proof. Let

$$\mathbf{M}_\alpha = \left[\begin{array}{c|c} \mathbf{A}_\alpha + \mathbf{D}^\alpha_\mathbf{2} & \mathbf{D}^\alpha_\mathbf{2} \\ \hline \mathbf{D}^\alpha_\mathbf{2} & \mathbf{A}_\alpha + \mathbf{D}^\alpha_\mathbf{-2} \end{array}\right] \tag{5.25}$$

be the Monsky matrix corresponding to α. We use induction to prove that $s(n) = 0$ and n is non-congruent. We begin by considering the case where α is multiplied by a single prime, s_{d+1}, satisfying the pattern of Legendre symbols described in the theorem statement, so

$$n_1 = \alpha s_{d+1}.$$

The $(2\delta + 2d + 2) \times (2\delta + 2d + 2)$ Monsky matrix for n_1 can be written as

$$\mathbf{M_{n_1}} = \left[\begin{array}{c|c} \mathbf{A_{n_1}} + \mathbf{D_2^{n_1}} & \mathbf{D_2^{n_1}} \\ \hline \mathbf{D_2^{n_1}} & \mathbf{A_{n_1}} + \mathbf{D_{-2}^{n_1}} \end{array}\right] = \left[\begin{array}{c|c||c|c} \mathbf{F} & \mathbf{v} & \mathbf{D_2^{\alpha}} & \mathbf{0} \\ \hline \mathbf{v}^T & 1 & \mathbf{0} & 0 \\ \hline\hline \mathbf{D_2^{\alpha}} & \mathbf{0} & \mathbf{C} & \mathbf{v} \\ \hline \mathbf{0} & 0 & \mathbf{v}^T & 1 \end{array}\right],$$

where $\mathbf{v}$ is a column vector with only a single element equal to one and all of its remaining elements equal to zero. Due to the form of $\mathbf{v}$, we introduce the matrices $\mathbf{F}$ and $\mathbf{C}$, where

$$\mathbf{F} = \mathbf{A}_\alpha + \mathbf{D_2^{\alpha}} + \mathbf{v}\mathbf{v}^T$$

and

$$\mathbf{C} = \mathbf{A}_\alpha + \mathbf{D_{-2}^{\alpha}} + \mathbf{v}\mathbf{v}^T.$$

Notice that $\mathbf{F}$ is nearly identical to the $\mathbf{A}_\alpha + \mathbf{D_2^{\alpha}}$ block in $\mathbf{M}_\alpha$, with the only difference between them being a single element along their main diagonals. This difference is a consequence of the column vector $\mathbf{v}$ having a single element equal to one. Likewise, the only difference between the $\mathbf{C}$ block in $\mathbf{M_{n_1}}$ and the $\mathbf{A}_\alpha + \mathbf{D_{-2}^{\alpha}}$ block in $\mathbf{M}_\alpha$ is a single element along their diagonals.

We carry out row and column operations on $\mathbf{M_{n_1}}$ to reduce it, so that its determinant can be easily computed. Let $m_{\epsilon\gamma}$ denote the entry in row ϵ and column γ of $\mathbf{M_{n_1}}$, and consider the element $m_{\epsilon\gamma} = 1$ with $\gamma = (\delta + d + 1)$ and $\epsilon \in [1, \delta + d]$. We subtract column $(\delta + d + 1)$ from column ϵ, and then subtract row $(\delta + d + 1)$ from row ϵ. Similarly, there is a single element $m_{\epsilon\gamma} = 1$ in $\mathbf{M_{n_1}}$ with $\gamma = (2\delta + 2d + 2)$ and $\epsilon \in [\delta + d + 2, 2\delta + 2d + 1]$. By subtracting column $(2\delta + 2d + 2)$ from column ϵ, and then subtracting row $(2\delta + 2d + 2)$ from row ϵ, we transform $\mathbf{M_{n_1}}$ into

$$\mathbf{M^*_{n_1}} = \left[\begin{array}{c|c||c|c} \mathbf{A}_\alpha + \mathbf{D_2^{\alpha}} & \mathbf{0} & \mathbf{D_2^{\alpha}} & \mathbf{0} \\ \hline \mathbf{0} & 1 & \mathbf{0} & 0 \\ \hline\hline \mathbf{D_2^{\alpha}} & \mathbf{0} & \mathbf{A}_\alpha + \mathbf{D_{-2}^{\alpha}} & \mathbf{0} \\ \hline \mathbf{0} & 0 & \mathbf{0} & 1 \end{array}\right].$$

Applying row and column interchanges to $\mathbf{M}^{*}_{\mathbf{n_1}}$ allows us to write it as

$$\mathbf{M}^{**}_{\mathbf{n_1}} = \left[\begin{array}{c|c||c|c} \mathbf{A}_\alpha + \mathbf{D}^{\alpha}_{\mathbf{2}} & \mathbf{D}^{\alpha}_{\mathbf{2}} & \mathbf{0} & \mathbf{0} \\ \hline \mathbf{D}^{\alpha}_{\mathbf{2}} & \mathbf{A}_\alpha + \mathbf{D}^{\alpha}_{\mathbf{-2}} & \mathbf{0} & \mathbf{0} \\ \hline\hline \mathbf{0} & \mathbf{0} & 1 & 0 \\ \hline \mathbf{0} & \mathbf{0} & 0 & 1 \end{array}\right].$$

Since we are working over $\mathbb{F}_2$, and $\mathbf{M}^{**}_{\mathbf{n_1}}$ was obtained from $\mathbf{M}_{\mathbf{n_1}}$ via a series of elementary row and column operations, we have

$$\det(\mathbf{M}_{\mathbf{n_1}}) = \det(\mathbf{M}^{**}_{\mathbf{n_1}}). \tag{5.26}$$

Furthermore, Proposition 2.27 implies that

$$\det(\mathbf{M}^{**}_{\mathbf{n_1}}) = \det \left[\begin{array}{c|c} \mathbf{A}_\alpha + \mathbf{D}^{\alpha}_{\mathbf{2}} & \mathbf{D}^{\alpha}_{\mathbf{2}} \\ \hline \mathbf{D}^{\alpha}_{\mathbf{2}} & \mathbf{A}_\alpha + \mathbf{D}^{\alpha}_{\mathbf{-2}} \end{array}\right].$$

We combine this equation with Equations (5.25) and (5.26) to deduce that

$$\det(\mathbf{M}_{\mathbf{n_1}}) = \det(\mathbf{M}_\alpha).$$

By assumption, $s(\alpha) = 0$, so we know that the Monsky matrix corresponding to α has full rank. Thus, we conclude that $\mathbf{M}_{\mathbf{n_1}}$ also has full rank, and hence $s(n_1) = 0$ and $n_1 = \alpha s_{d+1}$ is a non-congruent number.

We now assume that the theorem statement is true for the integer $n_* = \alpha s_{d+1} s_{d+2} \cdots s_{t-2} s_{t-1}$ formed by appending a tail of $(t-d-1)$ primes satisfying the specified Legendre symbol conditions onto α. By assumption, we know that

$$s(n_*) = 0.$$

Consider the integer

$$n = (\alpha s_{d+1} s_{d+2} \cdots s_{t-2} s_{t-1}) s_t$$

that is generated by appending a single prime, s_t, satisfying the required Legendre symbol conditions onto n_*. Proving that n is non-congruent by knowing that n_* has $s(n_*) = 0$ is analogous to showing that n_1 is non-congruent when α satisfies $s(\alpha) = 0$. This is because in each of the cases, a single prime of the specified form is appended onto a number whose corresponding congruent number elliptic curve has 2-Selmer rank equal to zero. Thus, an identical argument to the one that was used to verify that n_1 is a non-congruent number can be applied here to deduce that $s(n) = 0$ and n is non-congruent. □

The families of non-congruent numbers generated by Cases I.1.A and I.1.B of Theorem 5.5 exhibit an interesting property that is summarized by the following corollary.

Corollary 5.7. *Let*

$$W \cup \{s_{d+1}, s_{d+2}, \dots, s_t\}$$

be a collection of distinct primes satisfying the hypotheses of either Case I.1.A or Case I.1.B in Theorem 5.5. Any product of integers from the set

$$H = \{\alpha, s_{d+1}, s_{d+2}, \dots, s_t\},$$

where α is given by Equation (5.6), is a non-congruent number.

Proof. Let λ be a product of integers belonging to the set H. If λ is a product of two or more of the primes $s_{d+1}, s_{d+2}, \dots, s_t$, but does not contain α, then λ is non-congruent by Theorem 5.2. If λ is a product of α and at least one of the remaining primes in H, then λ is guaranteed to be non-congruent by either Case I.1.A or Case I.1.B of Theorem 5.5. □

5.5 Examples of Odd Non-congruent Numbers Generated from Known Non-congruent Numbers

In this section, we provide a collection of non-conguent numbers satisfying the criterion described in Theorem 5.5. Any odd non-congruent number corresponding to an elliptic curve with 2-Selmer rank equal to zero can be extended to produce other non-congruent numbers by using Theorem 5.5. Since various Legendre symbol conditions are imposed upon the primes that are appended onto the existing non-congruent numbers, Dirichlet's theorem on primes in arithmetic progressions (Theorem 2.20) ensures that each case in Theorem 5.5 generates infinitely many non-congruent numbers. Depending on the prime divisors of the non-congruent number chosen for α, the numbers constructed by applying Theorem 5.5 to α may overlap with those described by other known families of non-congruent numbers. However, the numerical examples that we present in Tables 5.5, 5.6, 5.7, 5.8, and 5.9 clearly belong to new families of non-congruent numbers, because their prime factorizations differ from those in [2, 6, 11–13, 15–17, 24, 27, 28, 36, 37, 39, 40, 49, 58].

Appendix A offers insight into how Maple can be used to construct the non-congruent numbers listed in the tables in this section. In particular, the appendix provides the Maple code used to produce one of the numerical examples in Table 5.5.

We begin by using Case I.1 in Theorem 5.5 to generate new families of non-congruent numbers from existing families of non-congruent numbers. First, we consider Lagrange's paper [27], which describes many different families of non-congruent numbers containing a maximum of three odd prime factors. We apply Case I.1 of our extension theorem to two of Lagrange's families of non-congruent numbers.

The first family has the form qr, where $q \equiv 5 \pmod 8$ and $r \equiv 7 \pmod 8$, and the condition

$$\left(\frac{q}{r}\right) = -1$$

is satisfied. The numbers in the second family are a product of three prime factors, pqr, with $p \equiv 1 \pmod 8$, $q \equiv 5 \pmod 8$, and $r \equiv 7 \pmod 8$ satisfying

$$\left(\frac{p}{q}\right) = \left(\frac{p}{r}\right) = -1, \quad \left(\frac{q}{r}\right) = \left(\frac{q}{p}\right) = -1, \quad \text{or} \quad \left(\frac{r}{p}\right) = \left(\frac{r}{q}\right) = -1.$$

In Section 9 of [17], Goto states that the numbers belonging to either one of Lagrange's two families described above correspond to congruent number elliptic curves with 2-Selmer rank of zero. Therefore, new families of non-congruent numbers can be generated using Theorem 5.5 to extend these existing families of non-congruent numbers. Some numerical examples are given in Tables 5.5 and 5.6.

Furthermore, since the numbers described by Theorem 5.1 were shown to have congruent number elliptic curves with 2-Selmer rank equal to zero, Theorem 5.5 can be applied to these non-congruent numbers to produce infinitely many non-congruent numbers. Tables 5.5 and 5.6 include several numerical examples that extend some of the non-congruent numbers given in Table 5.1.

It is worthwhile to mention that it is possible to apply Theorem 5.5 to odd non-congruent numbers that do not belong to existing families of non-congruent numbers. For a given odd integer α, one can compute $s(\alpha)$ by using Monsky's formula. If $s(\alpha) = 0$, then infinitely many new non-congruent numbers can be generated by applying Theorem 5.5 to α. Tables 5.5 and 5.6 list a few numerical examples that extend a non-congruent number α that does not belong to a known family of non-congruent numbers but satisfies $s(\alpha) = 0$.

Table 5.5: Non-congruent numbers $n = \alpha s_{d+1}s_{d+2}\cdots s_t$ generated by Cases I.1.A and I.1.B of Theorem 5.5

Theorem		**Extension Tail $s_{d+1}s_{d+2}\cdots s_t$**	
Satisfied by α	α	**Case I.1.A**	**Case I.1.B**
Lagrange with $\left(\frac{q}{r}\right) = -1$	$5 \cdot 7$	$11 \cdot 179 \cdot 499 \cdot 2179 \cdot 2531 \cdot 2699 \cdot 21211 \cdot 38459 \cdot 43019 \cdot 148691$	$19 \cdot 59 \cdot 811 \cdot 1459 \cdot 1931 \cdot 2371 \cdot 2579 \cdot 13331 \cdot 14699 \cdot 65579 \cdot 164771$
Lagrange with $\left(\frac{p}{q}\right) = \left(\frac{p}{r}\right) = -1$	$17 \cdot 5 \cdot 7$	$179 \cdot 1019 \cdot 2531 \cdot 5779 \cdot 10259 \cdot 41771 \cdot 64891 \cdot 74699 \cdot 220579 \cdot 254899$	$19 \cdot 59 \cdot 1291 \cdot 3251 \cdot 5011 \cdot 23099 \cdot 33851 \cdot 41411 \cdot 45779 \cdot 77419$
Lagrange with $\left(\frac{r}{p}\right) = \left(\frac{r}{q}\right) = -1$	$41 \cdot 5 \cdot 7$	$379 \cdot 1171 \cdot 1451 \cdot 3259 \cdot 14891 \cdot 17011 \cdot 54251 \cdot 67979 \cdot 280219 \cdot 280499$	$59 \cdot 131 \cdot 419 \cdot 1931 \cdot 5659 \cdot 12011 \cdot 12659 \cdot 110459 \cdot 189251 \cdot 442139$
Lagrange with $\left(\frac{q}{r}\right) = \left(\frac{q}{p}\right) = -1$	$41 \cdot 29 \cdot 31$	$59 \cdot 107 \cdot 1619 \cdot 3203 \cdot 9371 \cdot 20771 \cdot 33923 \cdot 48523 \cdot 210187 \cdot 308051 \cdot 926227$	$83 \cdot 139 \cdot 1499 \cdot 6067 \cdot 7043 \cdot 9931 \cdot 13171 \cdot 19843 \cdot 32939 \cdot 285451$
Theorem 5.1	$19 \cdot 11 \cdot 163 \cdot 419 \cdot 97 \cdot 313 \cdot 617$	$6011 \cdot 11867 \cdot 69931 \cdot 83339 \cdot 133387 \cdot 236339$	$811 \cdot 8059 \cdot 45979 \cdot 64451 \cdot 131779 \cdot 454379 \cdot 562091$
Theorem 5.1	$347 \cdot 83 \cdot 11 \cdot 3 \cdot 499 \cdot 1123 \cdot 2803 \cdot 673 \cdot 2953$	$140827 \cdot 172507 \cdot 191227 \cdot 670099$	$5051 \cdot 43787 \cdot 46691 \cdot 147179 \cdot 1174091$
Theorem 5.1	$11 \cdot 59 \cdot 163 \cdot 307 \cdot 947 \cdot 41 \cdot 1361 \cdot 2017$	$4651 \cdot 15139 \cdot 68611 \cdot 119827 \cdot 186019 \cdot 356731$	$6947 \cdot 12547 \cdot 43403 \cdot 149027 \cdot 119027 \cdot 696827 \cdot 783779$
Theorem 5.1	$3 \cdot 11 \cdot 67 \cdot 163 \cdot 691 \cdot 1483 \cdot 3019 \cdot 2179 \cdot 16987 \cdot 2137 \cdot 4273$	$23203 \cdot 121531 \cdot 938491 \cdot 1529851$	$27299 \cdot 137363 \cdot 1557443 \cdot 1734827$
Theorem 5.1	$3 \cdot 11 \cdot 19 \cdot 43 \cdot 59 \cdot 5 \cdot 13 \cdot 29 \cdot 37 \cdot 27481$	$124459 \cdot 376819 \cdot 467899 \cdot 589579$	$73259 \cdot 159059 \cdot 86291 \cdot 394811 \cdot 930179 \cdot 954971$
Theorem 5.1	$3 \cdot 19 \cdot 67 \cdot 83 \cdot 13 \cdot 61 \cdot 101 \cdot 149 \cdot 4177 \cdot 9649$	$138451 \cdot 172507 \cdot 290443 \cdot 731851$	$14771 \cdot 66491 \cdot 657947 \cdot 680003$
None	$13 \cdot 29 \cdot 37 \cdot 23 \cdot 31 \cdot 71$	$4003 \cdot 5867 \cdot 41947 \cdot 60779 \cdot 135131 \cdot 196387 \cdot 296299 \cdot 329891$	$2731 \cdot 3467 \cdot 1483 \cdot 16363 \cdot 32083 \cdot 76883 \cdot 269851 \cdot 274811 \cdot 659611$

Table 5.6: Non-congruent numbers $n = \alpha s_{d+1} s_{d+2} \cdots s_t$ generated by Cases I.1.C and I.1.D of Theorem 5.5

Theorem		**Extension Tail $s_{d+1}s_{d+2}\cdots s_t$**	
Satisfied by α	α	**Case I.1.C**	**Case I.1.D**
Lagrange with $\left(\frac{q}{r}\right) = -1$	$5 \cdot 7$	$3 \cdot 83 \cdot 467 \cdot 2243 \cdot 3923 \cdot 3947 \cdot 22067 \cdot 35363 \cdot 59723 \cdot 111443 \cdot 185363 \cdot 581843$	$43 \cdot 67 \cdot 107 \cdot 2027 \cdot 8563 \cdot 8803 \cdot 12923 \cdot 16363 \cdot 29803 \cdot 78467$
Lagrange with $\left(\frac{p}{q}\right) = \left(\frac{p}{r}\right) = -1$	$17 \cdot 5 \cdot 7$	$3 \cdot 227 \cdot 1907 \cdot 3947 \cdot 7643 \cdot 22307 \cdot 24443 \cdot 44483 \cdot 106907 \cdot 151787$	$107 \cdot 163 \cdot 547 \cdot 1187 \cdot 8803 \cdot 14387 \cdot 5987 \cdot 48563 \cdot 62563 \cdot 142907 \cdot 215723 \cdot 899467$
Lagrange with $\left(\frac{q}{r}\right) = \left(\frac{q}{p}\right) = -1$	$41 \cdot 29 \cdot 31$	$3 \cdot 11 \cdot 827 \cdot 1667 \cdot 6899 \cdot 28283 \cdot 47819 \cdot 80603 \cdot 179483 \cdot 453923$	$19 \cdot 1163 \cdot 1867 \cdot 2467 \cdot 2531 \cdot 9091 \cdot 32971 \cdot 71387 \cdot 93187 \cdot 203659$
Theorem 5.1	$19 \cdot 11 \cdot 163 \cdot 419 \cdot 97 \cdot 313 \cdot 617$	$211 \cdot 17027 \cdot 22739 \cdot 82387 \cdot 85571 \cdot 114659$	$1483 \cdot 15643 \cdot 26339 \cdot 60899 \cdot 174443 \cdot 191299 \cdot 396091 \cdot 235723$
None	$13 \cdot 29 \cdot 37 \cdot 23 \cdot 31 \cdot 71$	$827 \cdot 2683 \cdot 7451 \cdot 7963 \cdot 39827 \cdot 48563 \cdot 255443 \cdot 275923$	$2699 \cdot 3491 \cdot 8123 \cdot 27763 \cdot 21491 \cdot 121379 \cdot 133843 \cdot 156619$

We also provide some examples of non-congruent numbers that can be generated by Case II.2 of Theorem 5.5. The first family we extend is described by the following theorem from [40].

Theorem 5.8. *Let m be a fixed positive integer and let c be any integer satisfying $c \geq m$. Let T_m denote the set of positive integers with prime factorization $pr_1r_2 \cdots r_c$, where p is a prime of the form $8k+1$ and $r_1, r_2, \ldots, r_c$ are distinct primes of the form $8k+3$ such that*

$$\left(\frac{p}{r_i}\right) = \begin{cases} -1 & \textit{if } \ i = m, \\ 1 & \textit{if } i \neq m, \end{cases}$$

and

$$\left(\frac{r_j}{r_i}\right) = -1 \quad \textit{if} \quad j < i.$$

If $\alpha \in T_m$, then α is non-congruent.

The congruent number elliptic curves corresponding to the non-congruent numbers produced by this theorem are shown to have 2-Selmer rank equal to zero [40]. Therefore, Theorem 5.5 can be applied to these numbers to construct infinitely many new non-congruent numbers, including those listed in Table 5.7.

The non-congruent numbers generated by Case I.1 of Theorem 5.5 also correspond to congruent number elliptic curves with 2-Selmer rank equal to zero, so any of the numerical examples in Tables 5.5 and 5.6 can be extended by using Case II.2 of Theorem 5.5. We list several numerical examples in Table 5.7.

Table 5.7: Non-congruent numbers $n = \alpha s_{d+1}s_{d+2}\cdots s_t$ generated by Case II.2 of Theorem 5.5

Theorem Satisfied by $\boldsymbol{\alpha}$	$\boldsymbol{\alpha}$	**Case II.2 Extension Tail $\boldsymbol{s_{d+1}s_{d+2}\cdots s_t}$**	**Prime(s) $\boldsymbol{\mu \in T}$**
Theorem 5.8 with $m = 5$	$41 \cdot 43 \cdot 59 \cdot 107 \cdot 251 \cdot 547 \cdot 1307$	$3541 \cdot 15061 \cdot 31469 \cdot 52301 \cdot 595717 \cdot 703957$	41
Theorem 5.8 with $m = 5$	$41 \cdot 43 \cdot 59 \cdot 107 \cdot 251 \cdot 547 \cdot 1307$	$5381 \cdot 5717 \cdot 31357 \cdot 125101 \cdot 214189 \cdot 217981 \cdot 414157 \cdot 2844701$	107
Theorem 5.8 with $m = 5$	$41 \cdot 43 \cdot 59 \cdot 107 \cdot 251 \cdot 547 \cdot 1307$	$9157 \cdot 12517 \cdot 15773 \cdot 122069 \cdot 277741 \cdot 444557 \cdot 544877 \cdot 2836069$	41, 547, 1307
Theorem 5.8 with $m = 5$	$41 \cdot 43 \cdot 59 \cdot 107 \cdot 251 \cdot 547 \cdot 1307$	$8293 \cdot 9437 \cdot 13109 \cdot 84589 \cdot 119173 \cdot 251501 \cdot 687461 \cdot 2366173$	41, 43, 59, 107, 251, 547, 1307
Theorem 5.5 Case I.1.A	$17 \cdot 5 \cdot 7 \cdot 179 \cdot 1019 \cdot 2531 \cdot 5779$	$541 \cdot 1229 \cdot 2069 \cdot 67349 \cdot 405749 \cdot 671269 \cdot 786941 \cdot 838429$	17
Theorem 5.5 Case I.1.A	$17 \cdot 5 \cdot 7 \cdot 179 \cdot 1019 \cdot 2531 \cdot 5779$	$5557 \cdot 17477 \cdot 58733 \cdot 114197 \cdot 128813 \cdot 136237 \cdot 337973 \cdot 529157$	5, 7, 179, 2531, 5779
Theorem 5.5 Case I.1.A	$17 \cdot 5 \cdot 7 \cdot 179 \cdot 1019 \cdot 2531 \cdot 5779$	$3533 \cdot 18133 \cdot 51133 \cdot 64333 \cdot 77797 \cdot 372277$	17, 5, 7, 179, 1019, 2531, 5779
None	$13 \cdot 29 \cdot 37 \cdot 23 \cdot 31 \cdot 71$	$877 \cdot 4877 \cdot 8933 \cdot 9397 \cdot 15173 \cdot 125197 \cdot 414629 \cdot 495133$	13
None	$13 \cdot 29 \cdot 37 \cdot 23 \cdot 31 \cdot 71$	$173 \cdot 4813 \cdot 6269 \cdot 58237 \cdot 60733 \cdot 94709 \cdot 140773 \cdot 353053$	71
None	$13 \cdot 29 \cdot 37 \cdot 23 \cdot 31 \cdot 71$	$4013 \cdot 6917 \cdot 12373 \cdot 14869 \cdot 23981 \cdot 157141 \cdot 414413 \cdot 429701$	29, 37, 23
None	$13 \cdot 29 \cdot 37 \cdot 23 \cdot 31 \cdot 71$	$709 \cdot 13037 \cdot 14029 \cdot 21221 \cdot 68141 \cdot 79669 \cdot 80221 \cdot 347813 \cdot 1186621 \cdot 2773613$	13, 37, 23, 31, 71

Finally, we provide some examples of non-congruent numbers generated by Cases III.2 and III.3 of Theorem 5.5. The non-congruent numbers α, described by Theorems 5.2, 5.3, and 5.4, have $s(\alpha) = 0$. This means that we can apply Cases III.2 and III.3 of Theorem 5.5 to these numbers. In addition, since the non-congruent numbers listed in Tables 5.5, 5.6, and 5.7 correspond to elliptic curves with 2-Selmer rank equal to zero, it is possible to append a tail of primes of the form described in either Case III.2 or Case III.3 of Theorem 5.5 onto any of the numbers in Tables 5.5, 5.6, and 5.7 to produce new non-congruent numbers. Examples of non-congruent numbers that result from applying Case III.2 of our extension theorem to non-congruent numbers given by Theorems 5.2, 5.3, and 5.4, and to a couple numbers from Tables 5.5 and 5.7 are listed in Table 5.8.

Table 5.8: Non-congruent numbers $n = \alpha s_{d+1} s_{d+2} \cdots s_t$ generated by Case III.2 of Theorem 5.5

Theorem Satisfied by $\boldsymbol{\alpha}$	$\boldsymbol{\alpha}$	**Case III.2 Extension Tail $\boldsymbol{s_{d+1}s_{d+2}\cdots s_t}$**	**Prime(s) $\boldsymbol{\mu \in T}$**
Theorem 5.2	$19 \cdot 11 \cdot 163 \cdot 419$	$1361 \cdot 1889 \cdot 2833 \cdot 14401 \cdot 44497 \cdot 79537 \cdot 98689 \cdot 217169 \cdot 250433 \cdot 969041$	19, 11, 419
Theorem 5.3	$11 \cdot 59 \cdot 163 \cdot 307 \cdot 947$	$809 \cdot 1009 \cdot 5881 \cdot 8681 \cdot 58153 \cdot 124673 \cdot 361961 \cdot 435401$	11, 59, 163, 307, 947
Theorem 5.4	$3 \cdot 19 \cdot 67 \cdot 83 \cdot 13 \cdot 61 \cdot 101 \cdot 149$	$16481 \cdot 46049 \cdot 70937 \cdot 78233 \cdot 521777 \cdot 1387649$	3, 19, 67, 83, 61, 101, 149
None	$13 \cdot 29 \cdot 37 \cdot 23 \cdot 31 \cdot 71$	$8017 \cdot 24337 \cdot 31121 \cdot 49481 \cdot 81689 \cdot 214033 \cdot 532801 \cdot 1265393$	71
Theorem 5.5 Case I.1.A	$41 \cdot 29 \cdot 31 \cdot 59 \cdot 107 \cdot 1619$	$1801 \cdot 2393 \cdot 6841 \cdot 9001 \cdot 23057 \cdot 75041 \cdot 289841 \cdot 1225297$	41, 29, 31, 59, 1619
Theorem 5.5 Case II.2	$17 \cdot 5 \cdot 7 \cdot 179 \cdot 1019 \cdot 2531 \cdot 5779 \cdot 3533 \cdot 18133$	$56401 \cdot 88321 \cdot 189961 \cdot 191969 \cdot 551321 \cdot 1669649$	17, 2531, 18133

Because Case III.3 of Theorem 5.5 is a generalization of Theorem 5.1, the non-congruent numbers, n, listed in Table 5.1 that arise from applying Theorem 5.1 to the non-congruent numbers, α, produced by Theorems 5.2, 5.3, and 5.4 can also be generated by Case III.3 of Theorem 5.5. Therefore, the examples that we list in Table 5.9 are constructed by applying Case III.3 of Theorem 5.5 to a few of the numbers in Tables 5.5, 5.6, and 5.7. Note that the numbers in Table 5.9 cannot be produced by Theorem 5.1.

Table 5.9: Non-congruent numbers $n = \alpha s_{d+1} s_{d+2} \cdots s_t$ generated by applying Case III.3 of Theorem 5.5 to numbers in Tables 5.5, 5.6, and 5.7

$\boldsymbol{\alpha}$	**Case III.3 Extension Tail $\boldsymbol{s_{d+1} s_{d+2} \cdots s_t}$**	**Extension Tail Legendre Symbols that Equal -1**
$13 \cdot 29 \cdot 37 \cdot 23 \cdot 31 \cdot 71$	$593 \cdot 521 \cdot 857 \cdot 6977 \cdot 38561 \cdot 36433 \cdot 75193 \cdot 56377 \cdot 54833 \cdot 331553$	$\left(\frac{593}{13}\right)$, $\left(\frac{521}{23}\right)$, $\left(\frac{857}{37}\right)$, $\left(\frac{6977}{29}\right)$, $\left(\frac{38561}{521}\right)$, $\left(\frac{36433}{13}\right)$, $\left(\frac{75193}{38561}\right)$, $\left(\frac{56377}{521}\right)$, $\left(\frac{54833}{71}\right)$, $\left(\frac{331553}{75193}\right)$
$17 \cdot 5 \cdot 7 \cdot 179 \cdot 1019 \cdot 2531 \cdot 5779$	$5881 \cdot 7561 \cdot 7841 \cdot 7481 \cdot 12601 \cdot 59921 \cdot 28729 \cdot 47681 \cdot 324361$	$\left(\frac{5881}{2531}\right)$, $\left(\frac{7561}{1019}\right)$, $\left(\frac{7841}{1019}\right)$, $\left(\frac{7481}{7}\right)$, $\left(\frac{12601}{179}\right)$, $\left(\frac{59921}{5881}\right)$, $\left(\frac{28729}{7841}\right)$, $\left(\frac{47681}{28729}\right)$, $\left(\frac{324361}{5881}\right)$
$5 \cdot 7 \cdot 43 \cdot 67 \cdot 107 \cdot 2027$	$4649 \cdot 5009 \cdot 2801 \cdot 18289 \cdot 19001 \cdot 20441 \cdot 56809 \cdot 62969 \cdot 221729$	$\left(\frac{4649}{43}\right)$, $\left(\frac{5009}{67}\right)$, $\left(\frac{2801}{5009}\right)$, $\left(\frac{18289}{7}\right)$, $\left(\frac{19001}{7}\right)$, $\left(\frac{20441}{18289}\right)$, $\left(\frac{56809}{5009}\right)$, $\left(\frac{62969}{2027}\right)$, $\left(\frac{221729}{19001}\right)$
$17 \cdot 5 \cdot 7 \cdot 179 \cdot 1019 \cdot 2531 \cdot 5779 \cdot 541 \cdot 1229$	$2129 \cdot 7481 \cdot 5849 \cdot 44641 \cdot 59921 \cdot 39089 \cdot 70289 \cdot 710873$	$\left(\frac{2129}{179}\right)$, $\left(\frac{7481}{7}\right)$, $\left(\frac{5849}{7481}\right)$, $\left(\frac{44641}{1229}\right)$, $\left(\frac{59921}{1229}\right)$, $\left(\frac{39089}{17}\right)$, $\left(\frac{70289}{17}\right)$, $\left(\frac{710873}{5}\right)$

Notice that the different cases of Theorem 5.5 can be combined to generate new non-congruent numbers. This is illustrated by the numerical examples listed in the final row of Table 5.8 and Table 5.9 that apply Case I.1.A, Case II.2, and either Case III.2 or Case III.3 of Theorem 5.5 to produce non-congruent numbers.

Chapter 6

The Generation of Families of Even Non-congruent Numbers From Known Non-congruent Numbers

6.1 Overview

In this chapter, we present a criterion for generating new families of even non-congruent numbers. Our approach is similar to that described in Chapter 5 for producing families of odd non-congruent numbers. We construct infinitely many new even non-congruent numbers by appending primes of a certain form onto existing even non-congruent numbers, whose corresponding congruent number elliptic curves have 2-Selmer rank equal to zero. This allows us to generate even non-congruent numbers with arbitrarily many prime factors in each of the four odd congruence classes modulo eight. This characteristic distinguishes our result from other theorems on even non-congruent numbers that place restrictions on the prime divisors of the non-congruent numbers, only allowing an unlimited number of prime factors in at most two odd congruence classes modulo eight.

This chapter is based on results that appear in [42] and [43].

6.2 An Extension Technique for Generating New Families of Even Non-congruent Numbers

We begin by stating our main theorem. We let p_i, q_j, r_k, and s_l with $i, j, k, l \in \mathbb{N}^+$ be distinct odd primes, and let $a, b, c, d \in \mathbb{N}$ with $(a + b + c + d) > 0$. We define the set

$$P = \begin{cases} \emptyset & \text{if } a = 0, \\ \{p_1, p_2, \ldots, p_a\} & \text{if } a > 0. \end{cases}$$

The sets Q, R, and S with $|Q| = b, |R| = c$, and $|S| = d$ are defined analogously. In addition, we let

$$W = P \cup Q \cup R \cup S.$$

Theorem 6.1. *Define*

$$\beta = 2\left(\prod_{p_i \in P} p_i\right)\left(\prod_{q_j \in Q} q_j\right)\left(\prod_{r_k \in R} r_k\right)\left(\prod_{s_l \in S} s_l\right),$$

and suppose that the elliptic curve

$$y^2 = x(x^2 - \beta^2)$$

has 2-Selmer rank of zero. Let $t > d$ with $t \in \mathbb{N}^+$, and define the even square-free positive integer n by

$$n = \beta s_{d+1} s_{d+2} \cdots s_t,$$

where the odd prime factors of n satisfy the congruence conditions described in one of the four cases in Table 6.1.

Table 6.1: Congruence conditions for the odd prime factors of the even number n

Condition	$\boldsymbol{p_i}$**(mod 8)** $\forall\, \boldsymbol{p_i \in P}$	$\boldsymbol{q_j}$**(mod 8)** $\forall\, \boldsymbol{q_j \in Q}$	$\boldsymbol{r_k}$**(mod 8)** $\forall\, \boldsymbol{r_k \in R}$	$\boldsymbol{s_\gamma}$**(mod 8)** $\forall\, \boldsymbol{\gamma \in [1, t]}$
I	5	3	7	1
II	1	5	7	3
III	1	7	3	5
IV	1	5	3	7

In addition, assume that the primes appended onto β satisfy one of the following Legendre symbol conditions.

Condition 1:
For all $h, \sigma \in [d+1, t]$ with $h \neq \sigma$

$$\left(\frac{s_\sigma}{s_h}\right) = 1,$$

and define $T \subseteq W$ with

$$T = \left\{ \mu \;\middle|\; \left(\frac{s_h}{\mu}\right) = -1 \;\; \forall \;\; h \in [d+1, t] \right\}$$

and $|T| \equiv 1 \pmod 2$. For all primes $\varepsilon \in W \backslash T$,

$$\left(\frac{s_h}{\varepsilon}\right) = 1 \;\; \forall \;\; h \in [d+1, t].$$

Condition 2:
For each $h \in [d+1, t]$, the set L_h defined by

$$L_h = \left\{ \left(\frac{s_h}{p_i}\right), \left(\frac{s_h}{q_j}\right), \left(\frac{s_h}{r_k}\right), \left(\frac{s_h}{s_g}\right) \;\; \text{with } p_i \in P, q_j \in Q, r_k \in R, g \in [1, h) \right\}$$

has exactly one Legendre symbol equal to -1.

Condition 3:
For all $h \in [d+1, t]$, $p_i \in P$, $q_j \in Q$, $r_k \in R$, and $g \in [1, h)$, one of the following four sets of Legendre symbol conditions hold.

A) $$\left(\frac{s_h}{p_i}\right) = \left(\frac{s_h}{q_j}\right) = \left(\frac{s_h}{r_k}\right) = \left(\frac{s_h}{s_g}\right) = 1.$$

B) $$\left(\frac{s_h}{p_i}\right) = \left(\frac{s_h}{q_j}\right) = \left(\frac{s_h}{r_k}\right) = \left(\frac{s_h}{s_g}\right) = -1.$$

C) $$\left(\frac{p_i}{s_h}\right) = \left(\frac{q_j}{s_h}\right) = \left(\frac{r_k}{s_h}\right) = \left(\frac{s_g}{s_h}\right) = 1.$$

D) $$\left(\frac{p_i}{s_h}\right) = \left(\frac{q_j}{s_h}\right) = \left(\frac{r_k}{s_h}\right) = \left(\frac{s_g}{s_h}\right) = -1.$$

Condition 4:
Let $h \in [d+1, t]$, $\varepsilon \in \mathbb{N}^+$ and define $H \subseteq W$, where

$$|H| = \begin{cases} \text{Odd} & \text{if } (t-d) \equiv 0 \pmod 4, \\ 1 & \text{if } (t-d) \equiv 2 \pmod 4, \end{cases}$$

and $\mu \in H$ if

$$\left(\frac{\mu}{s_h}\right) = \begin{cases} 1 & \text{for } h = d + (2\varepsilon - 1), \\ -1 & \text{for } h = d + 2\varepsilon. \end{cases}$$

Set

$$\left(\frac{s_\sigma}{s_h}\right) = \left(\frac{\lambda}{s_h}\right) = 1$$

for all $h \in [d+1, t]$, $\sigma \in [d+1, h)$, and all primes $\lambda \in W \backslash H$.

Then, in each of the cases described in Table 6.2, n is a non-congruent number with $s(n) = 0$.

Table 6.2: Conditions on the primes in the extension tail of the even number n

Case	**Congruence Condition**	**Legendre Symbol Condition**	**Parity of $(t-d)$**
I.1	I	1	Even
I.2	I	2	No restriction
II.3	II	3.A, 3.B, 3.C, 3.D	Even
III.3.A	III	3.A	No restriction
IV.4	IV	4	Even

Our technique for proving this theorem utilizes theory from the field of linear algebra along with Monsky's formula for the 2-Selmer rank of E_n. We work over $\mathbb{F}_2$ and make use of Lemma 5.6 to simplify the calculations in our proof. As in Section 5.4, we set

$$\delta = (a+b+c) \qquad \text{and} \qquad \omega = (2\delta + t + d).$$

In addition, we let $\mathbf{A}_\beta$ denote the square $\mathbf{A}$ matrix of order $(\delta + d)$ for β, and $\mathbf{D}_\mathbf{2}^\beta$ and $\mathbf{D}_{\mathbf{-1}}^\beta$ represent the diagonal matrices corresponding to β; the entries in these matrices are defined in Theorem 3.15. We now work through the proofs of the cases described in Theorem 6.1 separately, beginning with Case I.1.

Case I.1 Proof. We use Equation (3.17) to form the $(2\delta + 2d) \times (2\delta + 2d)$ Monsky matrix,

$$\mathbf{M}_\mathbf{e}^\beta = \left[\begin{array}{c|c} \mathbf{D}_\mathbf{2}^\beta & \mathbf{A}_\beta + \mathbf{D}_\mathbf{2}^\beta \\ \hline {\mathbf{A}_\beta}^T + \mathbf{D}_\mathbf{2}^\beta & \mathbf{D}_{\mathbf{-1}}^\beta \end{array}\right],$$

for the even number β. By assumption $s(\beta) = 0$, so Equation (3.15) implies that $\mathbf{M}_\mathbf{e}^\beta$ has full rank.

We now consider $n = \beta s_{d+1} s_{d+2} \cdots s_t$ and construct its corresponding $\mathbf{A}$ matrix

$$\mathbf{A_n} = \left[\begin{array}{c|c} \mathbf{A}_\beta & \mathbf{B} \\ \hline \mathbf{B}^T & \mathbf{I_{t-d}} \end{array}\right],$$

where $(t-d)$ is even. Note that $\mathbf{B}$ is a $(\delta + d) \times (t-d)$ matrix containing rows with entries all equal to zero, except for an odd number of rows with elements all equal to one. Because $(t-d)$ is even, the entries along the diagonal in the upper left block of $\mathbf{A_n}$ are not affected by the elements in $\mathbf{B}$, so they remain the same as in $\mathbf{A}_\beta$. The matrix $\mathbf{B}^T$ has an odd number of columns with entries all equal to one, and so there is an identity block in the lower right corner of $\mathbf{A_n}$. Thus, the Monsky matrix corresponding to n can be written as

$$\mathbf{M_e} = \left[\begin{array}{c|c||c|c} \mathbf{D}^\beta_\mathbf{2} & \mathbf{0} & \mathbf{A}_\beta + \mathbf{D}^\beta_\mathbf{2} & \mathbf{B} \\ \hline \mathbf{0} & \mathbf{0_{t-d}} & \mathbf{B}^T & \mathbf{I_{t-d}} \\ \hline\hline \mathbf{A}_\beta{}^T + \mathbf{D}^\beta_\mathbf{2} & \mathbf{B} & \mathbf{D}^\beta_\mathbf{-1} & \mathbf{0} \\ \hline \mathbf{B}^T & \mathbf{I_{t-d}} & \mathbf{0} & \mathbf{0_{t-d}} \end{array}\right].$$

By applying Equation (5.10) from Lemma 5.6, $\mathbf{M_e}$ can be transformed into

$$\mathbf{M'_e} = \left[\begin{array}{c|c||c|c} \mathbf{D}^\beta_\mathbf{2} & \mathbf{A}_\beta + \mathbf{D}^\beta_\mathbf{2} & \mathbf{B} & \mathbf{0} \\ \hline \mathbf{A}_\beta{}^T + \mathbf{D}^\beta_\mathbf{2} & \mathbf{D}^\beta_\mathbf{-1} & \mathbf{0} & \mathbf{B} \\ \hline\hline \mathbf{0} & \mathbf{B}^T & \mathbf{I_{t-d}} & \mathbf{0_{t-d}} \\ \hline \mathbf{B}^T & \mathbf{0} & \mathbf{0_{t-d}} & \mathbf{I_{t-d}} \end{array}\right],$$

with

$$\det(\mathbf{M_e}) = \det(\mathbf{M'_e}).$$

Notice that the matrix $\mathbf{M'_e}$ is similar to $\mathbf{M^*_o}$ given by Equation (5.22) in the proof of Case II.2 of Theorem 5.5, with the only difference being the elements in the $(2\delta + 2d) \times (2\delta + 2d)$ blocks located in their upper left corners. Therefore, we can follow the process outlined in the proof of Case II.2 of Theorem 5.5 to reduce $\mathbf{M'_e}$ to a form where Proposition 2.27 can be applied. This allows us to deduce that

$$\det(\mathbf{M'_e}) = \det \left[\begin{array}{c|c} \mathbf{D}^\beta_\mathbf{2} & \mathbf{A}_\beta + \mathbf{D}^\beta_\mathbf{2} \\ \hline \mathbf{A}_\beta{}^T + \mathbf{D}^\beta_\mathbf{2} & \mathbf{D}^\beta_\mathbf{-1} \end{array}\right] = \det(\mathbf{M}^\beta_\mathbf{e}).$$

Since $\mathbf{M}_{\mathbf{e}}^{\beta}$ has full rank, its determinant is nonzero, so the above equation implies that $\mathbf{M}_{\mathbf{e}}'$ also has full rank. Thus, by Equation (3.15), we conclude that $s(n) = 0$ and n is non-congruent. □

We now verify that Case I.2 also yields non-congruent numbers. Note that this result is a generalization of Theorem 1.1 Case 1 in [42].

Case I.2 Proof. We use induction and follow a process analogous to that used in the proof of Case III.3 of Theorem 5.5. We begin by considering the integer

$$n' = \beta s_{d+1}$$

formed by appending the prime s_{d+1}, satisfying the specified pattern of Legendre symbols, onto the non-congruent number β. The $(2\delta + 2d + 2) \times (2\delta + 2d + 2)$ Monsky matrix for n' is

$$\mathbf{M}_{\mathbf{n}'} = \left[\begin{array}{c|c||c|c} \mathbf{D}_{\mathbf{2}}^{\beta} & \mathbf{0} & \mathbf{K} & \mathbf{v} \\ \hline \mathbf{0} & 0 & \mathbf{v}^T & 1 \\ \hline\hline \mathbf{K}^T & \mathbf{v} & \mathbf{D}_{\mathbf{-1}}^{\beta} & \mathbf{0} \\ \hline \mathbf{v}^T & 1 & \mathbf{0} & 0 \end{array}\right],$$

where $\mathbf{v}$ is a column vector containing $(\delta + d - 1)$ elements equal to zero and a single element equal to one, and

$$\mathbf{K} = \mathbf{A}_{\beta} + \mathbf{D}_{\mathbf{2}}^{\beta} + \mathbf{v}\mathbf{v}^T.$$

The matrix $\mathbf{M}_{\mathbf{n}'}$ can be transformed into

$$\mathbf{M}_{\mathbf{n}'}^{*} = \left[\begin{array}{c|c||c|c} \mathbf{D}_{\mathbf{2}}^{\beta} & \mathbf{A}_{\beta} + \mathbf{D}_{\mathbf{2}}^{\beta} & \mathbf{0} & \mathbf{0} \\ \hline {\mathbf{A}_{\beta}}^T + \mathbf{D}_{\mathbf{2}}^{\beta} & \mathbf{D}_{\mathbf{-1}}^{\beta} & \mathbf{0} & \mathbf{0} \\ \hline\hline \mathbf{0} & \mathbf{0} & 1 & 0 \\ \hline \mathbf{0} & \mathbf{0} & 0 & 1 \end{array}\right]$$

by carrying out similar row and column operations to those used in the proof of Case III.3 of Theorem 5.5 and applying Equation (5.9) from Lemma 5.6. Therefore, by Proposition 2.27, we have

$$\det(\mathbf{M}_{\mathbf{n}'}) = \det(\mathbf{M}_{\mathbf{n}'}^{*}) = \det(\mathbf{M}_{\mathbf{e}}^{\beta}).$$

By assumption $s(\beta) = 0$, so as in the proof for Case I.1 of Theorem 6.1, we can conclude that $s(n') = 0$ and n' is a non-congruent number. The remainder of the proof can be completed by following the process outlined in the proof of Case III.3 in Theorem 5.5. □

We now prove that Case II.3 generates non-congruent numbers. Note that Case II.3.A generalizes Theorem 1.2 in [42]. This is because Case II.3.A allows β to have arbitrarily many prime factors belonging to each odd congruence class modulo eight, whereas Theorem 1.2 in [42] imposes restrictions on the number of primes in certain odd congruence classes modulo eight.

Case II.3 Proof. The diagonal matrices for n are

$$\mathbf{D_2^n} = \left[\begin{array}{c|c} \mathbf{D_2^{\beta}} & \mathbf{0} \\ \hline \mathbf{0} & \mathbf{I_{t-d}} \end{array}\right] \qquad \text{and} \qquad \mathbf{D_{-1}^n} = \left[\begin{array}{c|c} \mathbf{D_{-1}^{\beta}} & \mathbf{0} \\ \hline \mathbf{0} & \mathbf{I_{t-d}} \end{array}\right]. \tag{6.1}$$

We consider the four subcases described in the theorem statement separately, beginning with Case II.3.A.

Case II.3.A:
By using Equation (3.14), we can write the **A** matrix corresponding to n as

$$\mathbf{A_n} = \left[\begin{array}{c|ccccc} \mathbf{A}_\beta & & & \mathbf{0} & & \\ \hline & a_{d+1} & 0 & \cdots & \cdots & 0 \\ & 1 & a_{d+2} & \ddots & & \vdots \\ \mathbf{T} & \vdots & \ddots & \ddots & \ddots & \vdots \\ & \vdots & & \ddots & a_{t-1} & 0 \\ & 1 & \cdots & \cdots & 1 & a_t \end{array}\right] = \left[\begin{array}{c|c} \mathbf{A}_\beta & \mathbf{0} \\ \hline \mathbf{T} & \mathbf{A}_* \end{array}\right], \tag{6.2}$$

where **T** is given by Equation (5.14). The diagonal entries in $\mathbf{A}_*$ are dependent upon the parity of the quantity $(c + d)$ and, since $(t - d)$ is even, it follows that

$$(a_{d+1}, a_{d+2}, \ldots, a_{t-1}, a_t) = \begin{cases} (0, 1, \ldots, 0, 1) & \text{if } (c + d) \text{ is even,} \\ (1, 0, \ldots, 1, 0) & \text{if } (c + d) \text{ is odd.} \end{cases}$$

The Monsky matrix for n can be written as

$$\mathbf{M_e} = \left[\begin{array}{c|c||c|c}
\mathbf{D}_{\mathbf{2}}^{\beta} & \mathbf{0} & \mathbf{A}_{\beta} + \mathbf{D}_{\mathbf{2}}^{\beta} & \mathbf{0} \\ \hline
\mathbf{0} & \mathbf{I_{t-d}} & \mathbf{T} & \mathbf{A}_{*} + \mathbf{I_{t-d}} \\ \hline\hline
\mathbf{A}_{\beta}{}^{T} + \mathbf{D}_{\mathbf{2}}^{\beta} & \mathbf{T}^{T} & \mathbf{D}_{\mathbf{-1}}^{\beta} & \mathbf{0} \\ \hline
\mathbf{0} & \mathbf{A}_{*}{}^{T} + \mathbf{I_{t-d}} & \mathbf{0} & \mathbf{I_{t-d}}
\end{array}\right]$$

by combining Equations (3.17), (6.1), and (6.2).

In the case where $(c+d)$ is even, we apply Equation (5.8) from Lemma 5.6 to $\mathbf{M_e}$ to obtain

$$\mathbf{M}_{\mathbf{e}}^{\blacktriangle} = \left[\begin{array}{c|c||c|c}
\mathbf{D}_{\mathbf{2}}^{\beta} & \mathbf{A}_{\beta} + \mathbf{D}_{\mathbf{2}}^{\beta} & \mathbf{0} & \mathbf{0} \\ \hline
\mathbf{A}_{\beta}{}^{T} + \mathbf{D}_{\mathbf{2}}^{\beta} & \mathbf{D}_{\mathbf{-1}}^{\beta} & \mathbf{0} & \mathbf{T}^{T} \\ \hline\hline
\mathbf{0} & \mathbf{0} & \mathbf{I_{t-d}} & \mathbf{A}_{*}{}^{T} + \mathbf{I_{t-d}} \\ \hline
\mathbf{0} & \mathbf{T} & \mathbf{A}_{*} + \mathbf{I_{t-d}} & \mathbf{I_{t-d}}
\end{array}\right],$$

with

$$\det(\mathbf{M_e}) = \det(\mathbf{M}_{\mathbf{e}}^{\blacktriangle}).$$

We modify this matrix by carrying out the set of $(t-d-1)$ row replacements listed in the proof of Case I.1.B of Theorem 5.5. These operations transform the $\mathbf{A}_{*}{}^{T} + \mathbf{I_{t-d}}$ block into the $(t-d)$ zero matrix, while leaving the other elements in $\mathbf{M}_{\mathbf{e}}^{\blacktriangle}$ unchanged. We then reduce the $\mathbf{T}$ block to the zero matrix by adding all of the final $(t-d)$ columns in $\mathbf{M}_{\mathbf{e}}^{\blacktriangle}$ to each of columns $(\delta+d+a+b+1)$ through $(2\delta+2d)$. The entries in the $\mathbf{T}^{T}$ block do not modify the elements in the $\mathbf{D}_{\mathbf{-1}}^{\beta}$ block, because we are adding an even number of columns to each of the aforementioned $(c+d)$ columns in $\mathbf{M}_{\mathbf{e}}^{\blacktriangle}$. Altogether, these operations change $\mathbf{M}_{\mathbf{e}}^{\blacktriangle}$ into

$$\mathbf{M}_{\mathbf{e}}^{\blacktriangle\blacktriangle} = \left[\begin{array}{c|c||c|c}
\mathbf{D}_{\mathbf{2}}^{\beta} & \mathbf{A}_{\beta} + \mathbf{D}_{\mathbf{2}}^{\beta} & \mathbf{0} & \mathbf{0} \\ \hline
\mathbf{A}_{\beta}{}^{T} + \mathbf{D}_{\mathbf{2}}^{\beta} & \mathbf{D}_{\mathbf{-1}}^{\beta} & \mathbf{0} & \mathbf{T}^{T} \\ \hline\hline
\mathbf{0} & \mathbf{0} & \mathbf{I_{t-d}} & \mathbf{0_{t-d}} \\ \hline
\mathbf{0} & \mathbf{0} & \mathbf{A}_{*} + \mathbf{I_{t-d}} & \mathbf{I_{t-d}}
\end{array}\right].$$

We apply Proposition 2.27 to $\mathbf{M}_{\mathbf{e}}^{\blacktriangle\blacktriangle}$ and, because the $(2t-2d) \times (2t-2d)$ block in the lower right corner of $\mathbf{M}_{\mathbf{e}}^{\blacktriangle\blacktriangle}$ is a lower triangular matrix with determinant equal to one, we are able to conclude that

$$\det(\mathbf{M_e}) = \det(\mathbf{M_e^{\blacktriangle\blacktriangle}}) = \det\left[\begin{array}{c|c} \mathbf{D_2^{\beta}} & \mathbf{A}_{\beta} + \mathbf{D_2^{\beta}} \\ \hline {\mathbf{A}_{\beta}}^{T} + \mathbf{D_2^{\beta}} & \mathbf{D_{-1}^{\beta}} \end{array}\right] = \det(\mathbf{M_e^{\beta}}).$$

Thus, it follows that $s(n) = 0$ and n is non-congruent when $(c+d)$ is even.

In the case where $(c+d)$ is odd, we transform $\mathbf{M_e}$ into

$$\mathbf{M_e^{\diamond}} = \left[\begin{array}{c|c||c|c} \mathbf{D_2^{\beta}} & \mathbf{A}_{\beta} + \mathbf{D_2^{\beta}} & \mathbf{0} & \mathbf{0} \\ \hline {\mathbf{A}_{\beta}}^{T} + \mathbf{D_2^{\beta}} & \mathbf{D_{-1}^{\beta}} & \mathbf{T}^{T} & \mathbf{0} \\ \hline\hline \mathbf{0} & \mathbf{T} & \mathbf{I_{t-d}} & \mathbf{A}_{*} + \mathbf{I_{t-d}} \\ \hline \mathbf{0} & \mathbf{0} & {\mathbf{A}_{*}}^{T} + \mathbf{I_{t-d}} & \mathbf{I_{t-d}} \end{array}\right] \tag{6.3}$$

by applying Equation (5.7) from Lemma 5.6. We need to reduce $\mathbf{M_e^{\diamond}}$ so that Property 2.27 can be used to calculate its determinant. We carry out the $(t-d-1)$ row operations stated in the proof of case 2 of Theorem 5.5 Case I.1.A to change the $\mathbf{A}_{*} + \mathbf{I_{t-d}}$ block in $\mathbf{M_e^{\diamond}}$ into the zero matrix. We also transform the $\mathbf{T}^{T}$ block into the zero matrix by adding rows $(2\delta + 2d + 1)$ through $(2\delta + d + t)$ to each of rows $(\delta + d + a + b + 1)$ through $(2\delta + 2d)$ in $\mathbf{M_e^{\diamond}}$. Upon completing these row operations, $\mathbf{M_e^{\diamond}}$ has the form

$$\mathbf{M_e^{\diamond\diamond}} = \left[\begin{array}{c|c||c|c} \mathbf{D_2^{\beta}} & \mathbf{A}_{\beta} + \mathbf{D_2^{\beta}} & \mathbf{0} & \mathbf{0} \\ \hline {\mathbf{A}_{\beta}}^{T} + \mathbf{D_2^{\beta}} & \mathbf{D_{-1}^{\beta}} & \mathbf{0} & \mathbf{0} \\ \hline\hline \mathbf{0} & \mathbf{T} & \mathbf{I_{t-d}} & \mathbf{0_{t-d}} \\ \hline \mathbf{0} & \mathbf{0} & {\mathbf{A}_{*}}^{T} + \mathbf{I_{t-d}} & \mathbf{I_{t-d}} \end{array}\right].$$

The remainder of the proof can be completed analogously to the case where $(c+d)$ is even, allowing us to reach the desired conclusion that $s(n) = 0$ and n is non-congruent when $(c+d)$ is odd.

Case II.3.B:

We recall Equation (3.14), and use it, along with the specified pattern of Legendre symbols corresponding to the primes appended onto β, to form the $\mathbf{A}$ matrix for n. This matrix can be written as

$$\mathbf{A_n} = \left[\begin{array}{c|ccccc} & 1 & \cdots & \cdots & \cdots & 1 \\ \mathbf{A}_\beta & \vdots & & & & \vdots \\ & 1 & \cdots & \cdots & \cdots & 1 \\ \hline & a_{d+1} & 1 & \cdots & \cdots & 1 \\ & 0 & a_{d+2} & \ddots & & \vdots \\ \mathbf{U} & \vdots & \ddots & \ddots & \ddots & \vdots \\ & \vdots & & \ddots & a_{t-1} & 1 \\ & 0 & \cdots & \cdots & 0 & a_t \end{array}\right] = \left[\begin{array}{c|ccc} & 1 & \cdots & 1 \\ \mathbf{A}_\beta & \vdots & & \vdots \\ & 1 & \cdots & 1 \\ \hline \mathbf{U} & \multicolumn{3}{c}{\mathbf{A}_*} \end{array}\right],$$

where $\mathbf{U}$ is given by Equation (5.15), and

$$(a_{d+1}, a_{d+2}, \ldots, a_{t-1}, a_t) = \begin{cases} (1, 0, \ldots, 1, 0) & \text{if } (a+b) \text{ is even,} \\ (0, 1, \ldots, 0, 1) & \text{if } (a+b) \text{ is odd.} \end{cases}$$

Note that there are an even number of ones in each row of the upper right block of $\mathbf{A_n}$. Because we are working over $\mathbb{F}_2$, the elements along the diagonal in the upper left block of $\mathbf{A_n}$ remain the same as those in $\mathbf{A}_\beta$. We form the Monsky matrix for n,

$$\mathbf{M_e} = \left[\begin{array}{c|c||c|c} \mathbf{D_2^\beta} & \mathbf{0} & \mathbf{A}_\beta + \mathbf{D_2^\beta} & \begin{matrix} 1 & \cdots & 1 \\ \vdots & & \vdots \\ 1 & \cdots & 1 \end{matrix} \\ \hline \mathbf{0} & \mathbf{I_{t-d}} & \mathbf{U} & \mathbf{A}_* + \mathbf{I_{t-d}} \\ \hline\hline {\mathbf{A}_\beta}^T + \mathbf{D_2^\beta} & \mathbf{U}^T & \mathbf{D_{-1}^\beta} & \mathbf{0} \\ \hline \begin{matrix} 1 & \cdots & 1 \\ \vdots & & \vdots \\ 1 & \cdots & 1 \end{matrix} & {\mathbf{A}_*}^T + \mathbf{I_{t-d}} & \mathbf{0} & \mathbf{I_{t-d}} \end{array}\right],$$

by using $\mathbf{A_n}$ and the diagonal matrices given by Equation (6.1).

We consider the case where $(a+b)$ is even and transform $\mathbf{M_e}$ into

$$\mathbf{M_e^{\blacktriangle}} = \left[\begin{array}{c|c||c|c}
\mathbf{D_2^{\beta}} & \mathbf{A}_\beta + \mathbf{D_2^{\beta}} & \begin{matrix}1 & \cdots & 1\\ \vdots & & \vdots \\ 1 & \cdots & 1\end{matrix} & \mathbf{0} \\ \hline
\mathbf{A}_\beta{}^T + \mathbf{D_2^{\beta}} & \mathbf{D_{-1}^{\beta}} & \mathbf{0} & \mathbf{U}^T \\ \hline\hline
\begin{matrix}1 & \cdots & 1\\ \vdots & & \vdots \\ 1 & \cdots & 1\end{matrix} & \mathbf{0} & \mathbf{I_{t-d}} & \mathbf{A}_*{}^T + \mathbf{I_{t-d}} \\ \hline
\mathbf{0} & \mathbf{U} & \mathbf{A}_* + \mathbf{I_{t-d}} & \mathbf{I_{t-d}}
\end{array}\right]$$

by applying Equation (5.8) from Lemma 5.6. We carry out the $(t-d-1)$ row replacement operations listed in the proof of case 2 of Theorem 5.5 Case I.1.A to reduce the $\mathbf{A}_*{}^T + \mathbf{I_{t-d}}$ block in $\mathbf{M_e^{\blacktriangle}}$ to the $(t-d)$ zero block. We then add all of the final $(t-d)$ rows in $\mathbf{M_e^{\blacktriangle}}$ to each of rows $(\delta+d+1)$ through $(\delta+d+a+b)$ to convert all of the entries in the $\mathbf{U}^T$ block to zeros. Finally, we reduce the block consisting entirely of ones in the upper right quadrant of $\mathbf{M_e^{\blacktriangle}}$ to the zero matrix by adding all of rows $(2\delta+2d+1)$ through $(2\delta+d+t)$ to each of the first $(\delta+d)$ rows in $\mathbf{M_e^{\blacktriangle}}$. This collection of row operations transforms $\mathbf{M_e^{\blacktriangle}}$ into

$$\mathbf{M_e^{\blacktriangle\blacktriangle}} = \left[\begin{array}{c|c||c|c}
\mathbf{D_2^{\beta}} & \mathbf{A}_\beta + \mathbf{D_2^{\beta}} & \mathbf{0} & \mathbf{0} \\ \hline
\mathbf{A}_\beta{}^T + \mathbf{D_2^{\beta}} & \mathbf{D_{-1}^{\beta}} & \mathbf{0} & \mathbf{0} \\ \hline\hline
\begin{matrix}1 & \cdots & 1\\ \vdots & & \vdots \\ 1 & \cdots & 1\end{matrix} & \mathbf{0} & \mathbf{I_{t-d}} & \mathbf{0_{t-d}} \\ \hline
\mathbf{0} & \mathbf{U} & \mathbf{A}_* + \mathbf{I_{t-d}} & \mathbf{I_{t-d}}
\end{array}\right]$$

and, since we are working over $\mathbb{F}_2$,

$$\det(\mathbf{M_e}) = \det(\mathbf{M_e^{\blacktriangle}}) = \det(\mathbf{M_e^{\blacktriangle\blacktriangle}}).$$

Applying Proposition 2.27 to $\mathbf{M_e^{\blacktriangle\blacktriangle}}$ allows us to determine that

$$\det(\mathbf{M_e^{\blacktriangle\blacktriangle}}) = \det\left[\begin{array}{c|c}
\mathbf{D_2^{\beta}} & \mathbf{A}_\beta + \mathbf{D_2^{\beta}} \\ \hline
\mathbf{A}_\beta{}^T + \mathbf{D_2^{\beta}} & \mathbf{D_{-1}^{\beta}}
\end{array}\right] = \det(\mathbf{M_e^{\beta}}).$$

The above determinant cannot be equal to zero because of our original assumption that $s(\beta) = 0$. Therefore, Equation (3.15) implies that $s(n) = 0$ and n is non-congruent when $(a + b)$ is even.

In the case where $(a + b)$ is odd, we use Equation (5.7) from Lemma 5.6 to transform $\mathbf{M}_{\mathbf{e}}$ into

$$\mathbf{M}_{\mathbf{e}}^{\diamond} = \left[\begin{array}{c|c||c|c} \mathbf{D}_{\mathbf{2}}^{\beta} & \mathbf{A}_{\beta} + \mathbf{D}_{\mathbf{2}}^{\beta} & \mathbf{0} & \begin{matrix} 1 & \cdots & 1 \\ \vdots & & \vdots \\ 1 & \cdots & 1 \end{matrix} \\ \hline {\mathbf{A}_{\beta}}^{T} + \mathbf{D}_{\mathbf{2}}^{\beta} & \mathbf{D}_{-\mathbf{1}}^{\beta} & \mathbf{U}^{T} & \mathbf{0} \\ \hline\hline \mathbf{0} & \mathbf{U} & \mathbf{I}_{\mathbf{t-d}} & \mathbf{A}_{*} + \mathbf{I}_{\mathbf{t-d}} \\ \hline \begin{matrix} 1 & \cdots & 1 \\ \vdots & & \vdots \\ 1 & \cdots & 1 \end{matrix} & \mathbf{0} & {\mathbf{A}_{*}}^{T} + \mathbf{I}_{\mathbf{t-d}} & \mathbf{I}_{\mathbf{t-d}} \end{array}\right],$$

with

$$\det(\mathbf{M}_{\mathbf{e}}) = \det(\mathbf{M}_{\mathbf{e}}^{\diamond}).$$

We carry out the $(t - d - 1)$ row operations listed in the proof of Theorem 5.5 Case I.1.B to convert the $\mathbf{A}_{*} + \mathbf{I}_{\mathbf{t-d}}$ block in $\mathbf{M}_{\mathbf{e}}^{\diamond}$ into the zero matrix. We then reduce all of the nonzero entries in the upper right quadrant of $\mathbf{M}_{\mathbf{e}}^{\diamond}$ to zero by performing analogous row operations to the ones that we used to transform $\mathbf{M}_{\mathbf{e}}^{\blacktriangle}$ into $\mathbf{M}_{\mathbf{e}}^{\blacktriangle\blacktriangle}$ in the case where $(a + b)$ is even. Completing the remaining portion of the proof can be done by simply following the series of steps outlined in case with $(a + b)$ even. Thus, regardless of the parity of the quantity $(a + b)$, $s(n) = 0$ and n is non-congruent.

Case II.3.C:

We use the pattern of Legendre symbols for the prime factors of n and Equations (3.14), (3.17), and (6.1) to construct the Monsky matrix for n.

This matrix has the form

$$\mathbf{M_e} = \left[\begin{array}{c|c||c|c}
\mathbf{D_2^{\beta}} & \mathbf{0} & \mathbf{A}_{\beta} + \mathbf{D_2^{\beta}} & \mathbf{T}^T \\
\hline
\mathbf{0} & \mathbf{I_{t-d}} & \mathbf{0} & \begin{array}{ccccc} 0 & 1 & \cdots & \cdots & 1 \\ 0 & 1 & \ddots & & \vdots \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ \vdots & & \ddots & 0 & 1 \\ 0 & \cdots & \cdots & 0 & 1 \end{array} \\
\hline\hline
\mathbf{A}_{\beta}{}^T + \mathbf{D_2^{\beta}} & \mathbf{0} & \mathbf{D_{-1}^{\beta}} & \mathbf{0} \\
\hline
\mathbf{T} & \begin{array}{ccccc} 0 & 0 & \cdots & \cdots & 0 \\ 1 & 1 & \ddots & & \vdots \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ \vdots & & \ddots & 0 & 0 \\ 1 & \cdots & \cdots & 1 & 1 \end{array} & \mathbf{0} & \mathbf{I_{t-d}}
\end{array}\right],$$

where $\mathbf{T}$ is given by Equation (5.14). Applying Equation (5.8) from Lemma 5.6 to $\mathbf{M_e}$ transforms it into

$$\mathbf{M_e^{\blacktriangle}} = \left[\begin{array}{c|c||c|c}
\mathbf{D_2^{\beta}} & \mathbf{A}_{\beta} + \mathbf{D_2^{\beta}} & \mathbf{T}^T & \mathbf{0} \\
\hline
\mathbf{A}_{\beta}{}^T + \mathbf{D_2^{\beta}} & \mathbf{D_{-1}^{\beta}} & \mathbf{0} & \mathbf{0} \\
\hline\hline
\mathbf{T} & \mathbf{0} & \mathbf{I_{t-d}} & \begin{array}{ccccc} 0 & 0 & \cdots & \cdots & 0 \\ 1 & 1 & \ddots & & \vdots \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ \vdots & & \ddots & 0 & 0 \\ 1 & \cdots & \cdots & 1 & 1 \end{array} \\
\hline
\mathbf{0} & \mathbf{0} & \begin{array}{ccccc} 0 & 1 & \cdots & \cdots & 1 \\ 0 & 1 & \ddots & & \vdots \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ \vdots & & \ddots & 0 & 1 \\ 0 & \cdots & \cdots & 0 & 1 \end{array} & \mathbf{I_{t-d}}
\end{array}\right].$$

By inspection, it is clear that the structure of this matrix is similar to the one in Equation (6.3). Therefore, an analogous process to that described in the proof of Theorem 6.1 Case II.3.A with odd $(c+d)$ can be implemented to deduce that $s(n)=0$ and n is a non-congruent number.

Case II.3.D:
We use the Legendre symbol values and Equation (3.14) to construct

$$\mathbf{A_n} = \left[\begin{array}{ccc|ccccc} \multicolumn{3}{c|}{\mathbf{A}_\beta} & \multicolumn{5}{c}{\mathbf{U}^T} \\ \hline 1 & \cdots & 1 & a_{d+1} & 0 & \cdots & \cdots & 0 \\ \vdots & & \vdots & 1 & a_{d+2} & \ddots & & \vdots \\ \vdots & & \vdots & \vdots & \ddots & \ddots & \ddots & \vdots \\ \vdots & & \vdots & \vdots & & \ddots & a_{t-1} & 0 \\ 1 & \cdots & 1 & 1 & \cdots & \cdots & 1 & a_t \end{array}\right] = \left[\begin{array}{ccc|c} \multicolumn{3}{c|}{\mathbf{A}_\beta} & \mathbf{U}^T \\ \hline 1 & \cdots & 1 & \\ \vdots & & \vdots & \mathbf{A}_* \\ 1 & \cdots & 1 & \end{array}\right],$$

where $\mathbf{U}^T$ is the transpose of the matrix described in Equation (5.15). Notice that the elements along the diagonal in $\mathbf{A}_*$ depend upon the parity of the quantity $(\delta+d)$, where

$$(a_{d+1}, a_{d+2}, \ldots, a_{t-1}, a_t) = \begin{cases} (1,0,\ldots,1,0) & \text{if } (\delta+d) \text{ is odd,} \\ (0,1,\ldots,0,1) & \text{if } (\delta+d) \text{ is even.} \end{cases}$$

It follows that the Monsky matrix for n has the form

$$\mathbf{M_e} = \left[\begin{array}{c|c|c|c} \mathbf{D}_\mathbf{2}^\beta & \mathbf{0} & \mathbf{A}_\beta + \mathbf{D}_\mathbf{2}^\beta & \mathbf{U}^T \\ \hline \mathbf{0} & \mathbf{I_{t-d}} & \begin{matrix} 1 & \cdots & 1 \\ \vdots & & \vdots \\ 1 & \cdots & 1 \end{matrix} & \mathbf{A}_* + \mathbf{I_{t-d}} \\ \hline\hline \mathbf{A}_\beta{}^T + \mathbf{D}_\mathbf{2}^\beta & \begin{matrix} 1 & \cdots & 1 \\ \vdots & & \vdots \\ 1 & \cdots & 1 \end{matrix} & \mathbf{D}_{\mathbf{-1}}^\beta & \mathbf{0} \\ \hline \mathbf{U} & \mathbf{A}_*{}^T + \mathbf{I_{t-d}} & \mathbf{0} & \mathbf{I_{t-d}} \end{array}\right].$$

When $(\delta+d)$ is odd, Equation (5.7) from Lemma 5.6 can be applied to rearrange the blocks in $\mathbf{M_e}$. The resulting matrix is similar in structure to $\mathbf{M}_\mathbf{e}^\blacktriangle$ in the proof of Theorem 6.1 Case II.3.B with $(a+b)$ even. Therefore, we can complete the proof of the case where $(\delta+d)$ is odd by following the procedural details described in the proof of Theorem 6.1 Case II.3.B with $(a+b)$ even.

Similarly, when $(\delta+d)$ is even, we transform $\mathbf{M_e}$ by using Equation (5.8) from Lemma 5.6. The remainder of the proof can be completed by following the process described in the proof of Theorem 6.1 Case II.3.B with $(a+b)$ odd.

Thus, $s(n) = 0$ and n is a non-congruent number irrespective of the parity of $(\delta + d)$. □

Next, we provide the proof of Case III.3.A.

Case III.3.A Proof. We form the $(2\delta + 2t) \times (2\delta + 2t)$ Monsky matrix for $n = \beta s_{d+1} s_{d+2} \cdots s_t$. This matrix is described by Equation (3.17) and can be written in the following general form

$$\mathbf{M_e} = \left[\begin{array}{c|c||c|c} \mathbf{D}_{\mathbf{2}}^{\beta} & \mathbf{0} & \mathbf{A}_{\beta} + \mathbf{D}_{\mathbf{2}}^{\beta} & \mathbf{0} \\ \hline \mathbf{0} & \mathbf{I_{t-d}} & \mathbf{0} & \mathbf{I_{t-d}} \\ \hline\hline {\mathbf{A}_{\beta}}^{T} + \mathbf{D}_{\mathbf{2}}^{\beta} & \mathbf{0} & \mathbf{D}_{\mathbf{-1}}^{\beta} & \mathbf{0} \\ \hline \mathbf{0} & \mathbf{I_{t-d}} & \mathbf{0} & \mathbf{0_{t-d}} \end{array}\right].$$

In addition, the $(\delta + t) \times (\delta + t)$ diagonal matrices $\mathbf{D_2}$ and $\mathbf{D_{-1}}$ that correspond to n are given by

$$\mathbf{D_2} = \left[\begin{array}{c||c} \mathbf{D}_{\mathbf{2}}^{\beta} & \mathbf{0} \\ \hline\hline \mathbf{0} & \mathbf{I_{t-d}} \end{array}\right] = \left[\begin{array}{c|c||c} \mathbf{0_{a+b}} & \mathbf{0} & \mathbf{0} \\ \hline \mathbf{0} & \mathbf{I_{c+d}} & \mathbf{0} \\ \hline\hline \mathbf{0} & \mathbf{0} & \mathbf{I_{t-d}} \end{array}\right]$$

and

$$\mathbf{D_{-1}} = \left[\begin{array}{c||c} \mathbf{D}_{\mathbf{-1}}^{\beta} & \mathbf{0} \\ \hline\hline \mathbf{0} & \mathbf{0_{t-d}} \end{array}\right] = \left[\begin{array}{c|c|c||c} \mathbf{0_a} & \mathbf{0} & \mathbf{0} & \mathbf{0} \\ \hline \mathbf{0} & \mathbf{I_{b+c}} & \mathbf{0} & \mathbf{0} \\ \hline \mathbf{0} & \mathbf{0} & \mathbf{0_d} & \mathbf{0} \\ \hline\hline \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0_{t-d}} \end{array}\right].$$

We apply Equation (5.10) from Lemma 5.6 to $\mathbf{M_e}$ to transform it into

$$\mathbf{M'_e} = \left[\begin{array}{c|c||c|c} \mathbf{D}_{\mathbf{2}}^{\beta} & \mathbf{A}_{\beta} + \mathbf{D}_{\mathbf{2}}^{\beta} & \mathbf{0} & \mathbf{0} \\ \hline {\mathbf{A}_{\beta}}^{T} + \mathbf{D}_{\mathbf{2}}^{\beta} & \mathbf{D}_{\mathbf{-1}}^{\beta} & \mathbf{0} & \mathbf{0} \\ \hline\hline \mathbf{0} & \mathbf{0} & \mathbf{I_{t-d}} & \mathbf{I_{t-d}} \\ \hline \mathbf{0} & \mathbf{0} & \mathbf{0_{t-d}} & \mathbf{I_{t-d}} \end{array}\right],$$

with

$$\det(\mathbf{M_e}) = \det(\mathbf{M'_e}).$$

Notice that the lower right corner square block of order $(2t-2d)$ is an upper triangular matrix with determinant equal to one. Therefore, by applying Proposition 2.27, we can determine that

$$\det(\mathbf{M_e}) = \det \left[\begin{array}{c|c} \mathbf{D_2^\beta} & \mathbf{A}_\beta + \mathbf{D_2^\beta} \\ \hline {\mathbf{A}_\beta}^T + \mathbf{D_2^\beta} & \mathbf{D_{-1}^\beta} \end{array}\right]. \tag{6.4}$$

The block matrix in Equation (6.4) is recognizable as the Monsky matrix corresponding to β. Recall that by assumption $s(\beta) = 0$. Therefore, Equation (3.15) implies that the Monsky matrix for β has full rank, so by Equation (6.4), we conclude that

$$\det(\mathbf{M_e}) \neq 0.$$

Thus, $s(n) = 0$ and n is a non-congruent number. □

Finally, we complete the proof of Theorem 6.1 by verifying that Case IV.4 produces families of non-congruent numbers.

Case IV.4 Proof. First, we construct the diagonal matrices for n. Because the primes appended onto β are of the form $8k + 7$,

$$\mathbf{D_2^n} = \left[\begin{array}{c|c} \mathbf{D_2^\beta} & \mathbf{0} \\ \hline \mathbf{0} & \mathbf{0_{t-d}} \end{array}\right] \qquad \text{and} \qquad \mathbf{D_{-1}^n} = \left[\begin{array}{c|c} \mathbf{D_{-1}^\beta} & \mathbf{0} \\ \hline \mathbf{0} & \mathbf{I_{t-d}} \end{array}\right].$$

We define

$$\mathbf{u} = \left[\begin{array}{cccccc} 1 & 0 & \cdots & 1 & 0 \end{array}\right] \tag{6.5}$$

and

$$\mathbf{v} = \left[\begin{array}{cccccc} 0 & 1 & \cdots & 0 & 1 \end{array}\right] \tag{6.6}$$

to be a pair of row vectors containing $(t-d)$ elements that alternate between ones and zeros. The Monsky matrix for n can be written as

$$\mathbf{M_e} = \left[\begin{array}{c|c||c|c}
\mathbf{D_2^{\beta}} & \mathbf{0} & \mathbf{E} & \mathbf{F} \\ \hline
\mathbf{0} & \mathbf{0_{t-d}} & \mathbf{G} & \begin{matrix} 1 & 1 & \cdots & \cdots & 1 \\ 0 & 1 & \ddots & & \vdots \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ \vdots & & \ddots & 1 & 1 \\ 0 & \cdots & \cdots & 0 & 1 \end{matrix} \\ \hline\hline
\mathbf{E}^T & \mathbf{G}^T & \mathbf{D}^{\beta}_{\mathbf{-1}} & \mathbf{0} \\ \hline
\mathbf{F}^T & \begin{matrix} 1 & 0 & \cdots & \cdots & 0 \\ 1 & 1 & \ddots & & \vdots \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ \vdots & & \ddots & 1 & 0 \\ 1 & \cdots & \cdots & 1 & 1 \end{matrix} & \mathbf{0} & \mathbf{I_{t-d}}
\end{array}\right], \tag{6.7}$$

where the structure of the blocks $\mathbf{E}$, $\mathbf{F}$, and $\mathbf{G}$ vary depending on whether $(t-d) \equiv 2 \pmod 4$ or $(t-d) \equiv 0 \pmod 4$.

If $(t-d) \equiv 2 \pmod 4$, $\mathbf{G}$ is a $(t-d) \times (\delta + d)$ matrix with all of its elements equal to zero, except for a single column of the form $\mathbf{v}^T$, where $\mathbf{v}$ is given by Equation (6.6). The structure of $\mathbf{G}$ is important, because it ensures that the block immediately to the right of $\mathbf{G}$ has nonzero determinant; if $\mathbf{G}$ had simply been the zero matrix, then the upper triangular block situated beside $\mathbf{G}$ would have exhibited an alternating pattern of ones and zeros along its diagonal. The significance of this upper triangular block with nonzero determinant becomes apparent later in the proof when we apply Proposition 2.27.

When $(t-d) \equiv 2 \pmod 4$, the structure of the matrix $\mathbf{F}$ is dependent upon the prime that belongs to the set H. If $p_i \in H$ for any $i \in [1,a]$ or $q_j \in H$ for any $j \in [1,b]$, then $\mathbf{F}$ has $(c+d)$ rows of ones, $(a+b-1)$ rows of zeros, and a single row of the form $\mathbf{v}$. Similarly, if $r_k \in H$ for any $k \in [1,c]$ or $s_l \in H$ for any $l \in [1,d]$, then $\mathbf{F}$ has $(a+b)$ rows of zeros, $(c+d-1)$ rows of ones, and a single row of the form $\mathbf{u}$, where $\mathbf{u}$ is given by Equation (6.5). The rows in $\mathbf{F}$ that are composed either entirely of zeros or entirely of ones do not affect the elements along the diagonal in the block $\mathbf{E}$, because we are working over $\mathbb{F}_2$ and $(t-d)$ is even. The remaining row in $\mathbf{F}$ of the form $\mathbf{u}$ or $\mathbf{v}$ contains an odd number of ones because $(t-d) \equiv 2 \pmod 4$. Therefore, the block $\mathbf{E}$ is nearly identical to $\mathbf{A}_\beta + \mathbf{D}_{\mathbf{2}}^{\beta}$, with the only difference between these two matrices being a single element along their main diagonals.

We now use Equation (5.9) from Lemma 5.6 to transform $\mathbf{M_e}$ into

$$\mathbf{M}_{\mathbf{e}}^{*} = \left[\begin{array}{c|c||c|c}
\mathbf{D}_{\mathbf{2}}^{\beta} & \mathbf{E} & \mathbf{0} & \mathbf{F} \\ \hline
\mathbf{E}^{T} & \mathbf{D}_{\mathbf{-1}}^{\beta} & \mathbf{G}^{T} & \mathbf{0} \\ \hline\hline
\mathbf{F}^{T} & \mathbf{0} & \begin{matrix} 1 & 0 & \cdots & \cdots & 0 \\ 1 & 1 & \ddots & & \vdots \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ \vdots & & \ddots & 1 & 0 \\ 1 & \cdots & \cdots & 1 & 1 \end{matrix} & \mathbf{I}_{\mathbf{t-d}} \\ \hline
\mathbf{0} & \mathbf{G} & \mathbf{0}_{\mathbf{t-d}} & \begin{matrix} 1 & 1 & \cdots & \cdots & 1 \\ 0 & 1 & \ddots & & \vdots \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ \vdots & & \ddots & 1 & 1 \\ 0 & \cdots & \cdots & 0 & 1 \end{matrix}
\end{array}\right]. \tag{6.8}$$

We convert the $\mathbf{G}$ block into the zero matrix by adding each of the final $(t-d)$ columns in $\mathbf{M}_{\mathbf{e}}^{*}$ to the column in $\mathbf{M}_{\mathbf{e}}^{*}$ whose final $(t-d)$ elements alternate between zeros and ones. This single column replacement operation transforms the block $\mathbf{E}$ into $\mathbf{A}_\beta + \mathbf{D}_{\mathbf{2}}^{\beta}$ and the matrix $\mathbf{M}_{\mathbf{e}}^{*}$ into

$$\mathbf{M}_{\mathbf{e}}^{**} = \left[\begin{array}{c|c||c|c}
\mathbf{D}_{\mathbf{2}}^{\beta} & \mathbf{A}_\beta + \mathbf{D}_{\mathbf{2}}^{\beta} & \mathbf{0} & \mathbf{F} \\ \hline
\mathbf{E}^{T} & \mathbf{D}_{-\mathbf{1}}^{\beta} & \mathbf{G}^{T} & \mathbf{0} \\ \hline\hline
\mathbf{F}^{T} & \mathbf{K} & \begin{matrix} 1 & 0 & \cdots & \cdots & 0 \\ 1 & 1 & \ddots & & \vdots \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ \vdots & & \ddots & 1 & 0 \\ 1 & \cdots & \cdots & 1 & 1 \end{matrix} & \mathbf{I}_{\mathbf{t-d}} \\ \hline
\mathbf{0} & \mathbf{0} & \mathbf{0}_{\mathbf{t-d}} & \begin{matrix} 1 & 1 & \cdots & \cdots & 1 \\ 0 & 1 & \ddots & & \vdots \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ \vdots & & \ddots & 1 & 1 \\ 0 & \cdots & \cdots & 0 & 1 \end{matrix}
\end{array}\right],$$

where $\mathbf{K}$ has a single column of ones and all of its remaining entries equal to zero.

We reduce the $\mathbf{G}^T$ block to the zero matrix by carrying out a single row replacement operation in $\mathbf{M}_{\mathbf{e}}^{**}$. Specifically, we add each of rows $(2\delta+2d+1)$ through $(2\delta+d+t)$ to the row in $\mathbf{M}_{\mathbf{e}}^{**}$ with nonzero entries in $\mathbf{G}^T$. Note that this row replacement operation also transforms $\mathbf{E}^T$ into $\mathbf{A}_\beta{}^T + \mathbf{D}_{\mathbf{2}}^\beta$, so $\mathbf{M}_{\mathbf{e}}^{**}$ becomes

$$\mathbf{M}_{\mathbf{e}}^{***} = \left[\begin{array}{c|c||c|c}
\mathbf{D}_{\mathbf{2}}^\beta & \mathbf{A}_\beta + \mathbf{D}_{\mathbf{2}}^\beta & \mathbf{0} & \mathbf{F} \\ \hline
\mathbf{A}_\beta{}^T + \mathbf{D}_{\mathbf{2}}^\beta & \mathbf{D}_{-\mathbf{1}}^\beta & \mathbf{0} & \mathbf{K}^T \\ \hline\hline
\mathbf{F}^T & \mathbf{K} & \begin{matrix} 1 & 0 & \cdots & \cdots & 0 \\ 1 & 1 & \ddots & & \vdots \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ \vdots & & \ddots & 1 & 0 \\ 1 & \cdots & \cdots & 1 & 1 \end{matrix} & \mathbf{I_{t-d}} \\ \hline
\mathbf{0} & \mathbf{0} & \mathbf{0_{t-d}} & \begin{matrix} 1 & 1 & \cdots & \cdots & 1 \\ 0 & 1 & \ddots & & \vdots \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ \vdots & & \ddots & 1 & 1 \\ 0 & \cdots & \cdots & 0 & 1 \end{matrix}
\end{array}\right], \tag{6.9}$$

with

$$\det(\mathbf{M_e}) = \det(\mathbf{M}_{\mathbf{e}}^{***}). \tag{6.10}$$

Applying Proposition 2.27 to $\mathbf{M}_{\mathbf{e}}^{***}$ twice allows us to deduce that

$$\begin{aligned}
\det(\mathbf{M}_{\mathbf{e}}^{***}) &= \det \left[\begin{array}{c|c||c}
\mathbf{D}_{\mathbf{2}}^\beta & \mathbf{A}_\beta + \mathbf{D}_{\mathbf{2}}^\beta & \mathbf{0} \\ \hline
\mathbf{A}_\beta{}^T + \mathbf{D}_{\mathbf{2}}^\beta & \mathbf{D}_{-\mathbf{1}}^\beta & \mathbf{0} \\ \hline\hline
\mathbf{F}^T & \mathbf{K} & \begin{matrix} 1 & 0 & \cdots & \cdots & 0 \\ 1 & 1 & \ddots & & \vdots \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ \vdots & & \ddots & 1 & 0 \\ 1 & \cdots & \cdots & 1 & 1 \end{matrix}
\end{array}\right] \\
&= \det \left[\begin{array}{c|c}
\mathbf{D}_{\mathbf{2}}^\beta & \mathbf{A}_\beta + \mathbf{D}_{\mathbf{2}}^\beta \\ \hline
\mathbf{A}_\beta{}^T + \mathbf{D}_{\mathbf{2}}^\beta & \mathbf{D}_{-\mathbf{1}}^\beta
\end{array}\right]. \qquad (6.11)
\end{aligned}$$

The square matrix of order $(2\delta{+}2d)$ immediately above is recognizable as the Monsky matrix corresponding to β. By assumption $s(\beta) = 0$, so Equation (3.15) implies that the Monsky matrix for β has nonzero determinant. This fact when coupled with Equations (6.10) and (6.11) enables us to deduce that

$$\det(\mathbf{M_e}) \neq 0.$$

Therefore, when $(t - d) \equiv 2 \pmod 4$, $s(n) = 0$ and n is a non-congruent number.

If $(t-d) \equiv 0 \pmod 4$, $|H|$ is odd, so the $\mathbf{G}$ matrix in Equation (6.7) has an odd number of columns of the form $\mathbf{v}^T$, where $\mathbf{v}$ is given by Equation (6.6), and all of the remaining entries in $\mathbf{G}$ are equal to zero. Since there are an odd number of columns of the form $\mathbf{v}^T$ in $\mathbf{G}$, the block immediately to the right of $\mathbf{G}$ in $\mathbf{M_e}$ is an upper triangular matrix with ones along its main diagonal.

Suppose that the number of primes p_i with $i \in [1, a]$ and q_j with $j \in [1, b]$ belonging to the set H is η, and the number of primes r_k with $k \in [1, c]$ and s_l with $l \in [1, d]$ in H is κ. Then $\eta + \kappa = |H|$, and $\mathbf{F}$ has $(a + b - \eta)$ rows of zeros, η rows of the form $\mathbf{v}$, $(c + d - \kappa)$ rows of ones, and κ rows of the form $\mathbf{u}$, where $\mathbf{u}$ is given by Equation (6.5). Since $\mathbf{u}$ and $\mathbf{v}$ are row vectors of length $(t-d)$ and $(t-d) \equiv 0 \pmod 4$, there are an even number of elements equal to one in each of these two vectors. Therefore, the entries in the rows of $\mathbf{F}$ do not affect the elements along the diagonal in the block $\mathbf{E}$ and

$$\mathbf{E} = \mathbf{A}_\beta + \mathbf{D}_\mathbf{2}^\beta.$$

We follow an analogous process to the one described in the case where $(t-d) \equiv 2 \pmod 4$ to verify that n is a non-congruent number when $(t-d) \equiv 0 \pmod 4$. First, we apply Equation (5.9) from Lemma 5.6 to transform $\mathbf{M_e}$ into the matrix $\mathbf{M_e^*}$, given by Equation (6.8). To reduce the $\mathbf{G}$ block in $\mathbf{M_e^*}$ to a zero block, we add all of the final $(t - d)$ columns in $\mathbf{M_e^*}$ to each of the $|H|$ columns in $\mathbf{M_e^*}$ whose final $(t - d)$ entries alternate between zeros and ones. This process does not alter the $\mathbf{A}_\beta + \mathbf{D}_\mathbf{2}^\beta$ block in $\mathbf{M_e^*}$ because we are adding all of the final $(t - d)$ columns of $\mathbf{M_e^*}$ to another column in $\mathbf{M_e^*}$, and each row in $\mathbf{F}$ has either no ones or an even number of ones. The column operations transform $\mathbf{M_e^*}$ into

$$\mathbf{M_e^{**}} = \left[\begin{array}{c|c|c|c}
\mathbf{D_2^\beta} & \mathbf{A}_\beta + \mathbf{D_2^\beta} & \mathbf{0} & \mathbf{F} \\
\hline
\mathbf{A}_\beta{}^T + \mathbf{D_2^\beta} & \mathbf{D_{-1}^\beta} & \mathbf{G}^T & \mathbf{0} \\
\hline\hline
\mathbf{F}^T & \mathbf{K} & \begin{array}{ccccc} 1 & 0 & \cdots & \cdots & 0 \\ 1 & 1 & \ddots & & \vdots \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ \vdots & & \ddots & 1 & 0 \\ 1 & \cdots & \cdots & 1 & 1 \end{array} & \mathbf{I_{t-d}} \\
\hline
\mathbf{0} & \mathbf{0} & \mathbf{0_{t-d}} & \begin{array}{ccccc} 1 & 1 & \cdots & \cdots & 1 \\ 0 & 1 & \ddots & & \vdots \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ \vdots & & \ddots & 1 & 1 \\ 0 & \cdots & \cdots & 0 & 1 \end{array}
\end{array}\right],$$

where $\mathbf{K}$ is a matrix with $|H|$ columns of ones and $(\delta + d - |H|)$ columns of zeros.

Next, we complete a series of $|H|$ row replacement operations to convert the $\mathbf{G}^T$ block to the zero matrix. This involves adding all of rows $(2\delta+2d+1)$ through $(2\delta + d + t)$ in $\mathbf{M_e^{**}}$ to each of the $|H|$ rows in $\mathbf{G}^T$ of the form $\mathbf{v}$. These row operations do not affect the $\mathbf{D_{-1}^\beta}$ or $\mathbf{A}_\beta{}^T + \mathbf{D_2^\beta}$ blocks in $\mathbf{M_e^{**}}$. Therefore, $\mathbf{M_e^{**}}$ is transformed into the matrix $\mathbf{M_e^{***}}$, given by Equation (6.9), where the $\mathbf{K}$ block has $|H|$ columns composed entirely of ones and all remaining columns composed entirely of zeros.

The rest of the proof of the case where $(t - d) \equiv 0 \pmod 4$ can be completed by following the steps outlined in the proof of the case with $(t - d) \equiv 2 \pmod 4$. Thus, when $(t - d) \equiv 0 \pmod 4$, we conclude that $s(n) = 0$ and n is non-congruent. □

6.3 Examples of Even Non-congruent Numbers Generated from Known Non-congruent Numbers

In this section, we provide examples of non-congruent numbers that are generated by Theorem 6.1. These numbers are specified by values of Legendre symbols, and hence Dirichlet's theorem on primes in arithmetic progressions (Theorem 2.20) guarantees that our theorem produces infinitely many non-congruent numbers. Of significance is the fact that any even non-congruent number β with $s(\beta) = 0$ can be extended to produce infinitely many non-congruent numbers by using Theorem 6.1. Depending on the value chosen for β, the numbers generated by applying Theorem 6.1 may belong to existing families of non-congruent numbers. However, the numerical examples presented in Tables 6.4, 6.5, 6.6, 6.7, and 6.8 are from new families of non-congruent numbers, because their prime factorizations differ from those of known families of even non-congruent numbers [2, 6, 11, 12, 15–17, 27, 37, 49].

It is worthwhile to mention that the non-congruent numbers listed in the tables in this section can be generated with the aid of the Maple code given in Appendix A.

We begin by considering some existing families of non-congruent numbers, so that we can apply Theorem 6.1 to construct new non-congruent numbers.

Lagrange describes several families of even non-congruent numbers with a maximum of three distinct odd prime factors [27]. We summarize some of his results in Table 6.3.

Table 6.3: Lagrange's non-congruent numbers of the form $\beta = 2pq$ or $2pqr$, where p, q, and r are distinct odd primes

	p (mod 8)	q (mod 8)	r (mod 8)	Legendre Symbol Conditions Imposed on the Odd Prime Factors of β
1)	3	3	–	None
2)	1	5	–	$\left(\frac{p}{q}\right) = -1$
3)	7	3	–	$\left(\frac{p}{q}\right) = 1$
4)	1	3	3	$\left(\frac{p}{q}\right) = -\left(\frac{p}{r}\right)$
5)	1	5	5	$\left(\frac{p}{q}\right) = -\left(\frac{p}{r}\right)$
6)	7	3	5	$\left(\frac{p}{q}\right) = \left(\frac{p}{r}\right)$
7)	7	7	5	$\left(\frac{p}{q}\right) = \left(\frac{p}{r}\right) = -\left(\frac{q}{r}\right)$
8)	1	7	3	$\left(\frac{p}{q}\right) = \left(\frac{p}{r}\right) = -1$ or $\left(\frac{r}{p}\right) = \left(\frac{r}{q}\right) = -1$

In Section 9 of [17], Goto asserts that numbers β of the form described by Table 6.3 correspond to congruent number elliptic curves with 2-Selmer rank equal to zero. Therefore, Theorem 6.1 can be used to extend these numbers to produce new families of even non-congruent numbers containing arbitrarily many distinct prime factors. In addition, since the even integers n described by Theorem 4.1 were proven to have $s(n) = 0$, they too can be extended by Theorem 6.1. In fact, any even non-congruent number n with $s(n) = 0$ can be extended to produce an infinite collection of non-congruent numbers by using Theorem 6.1.

We begin by applying Case I.1 of Theorem 6.1 to a few non-congruent numbers described by Lagrange's results in Table 6.3 and a non-congruent number that is listed in Table 4.1. The resulting numerical examples generated by Case I.1 of Theorem 6.1 are stated in Table 6.4.

Table 6.4: Non-congruent numbers $n = \beta s_{d+1}s_{d+2}\cdots s_t$ generated by Case I.1 of Theorem 6.1

Theorem Satisfied by β	$\boldsymbol{\beta}$	**Case I.1 Extension Tail $s_{d+1}s_{d+2}\cdots s_t$**	**Prime(s) $\mu \in T$**
Lagrange Case 1 in Table 6.3	$2\cdot 43\cdot 83$	$281\cdot 337\cdot 1433\cdot 1601\cdot 2593\cdot 4129\cdot 6529\cdot 17393\cdot 98737\cdot 337121\cdot 490001\cdot 2015033$	83
Lagrange Case 3 in Table 6.3	$2\cdot 23\cdot 11$	$89\cdot 97\cdot 881\cdot 1433\cdot 2777\cdot 22697\cdot 25793\cdot 37489\cdot 51217\cdot 149689$	23
Lagrange Case 6 in Table 6.3	$2\cdot 19\cdot 5\cdot 103$	$761\cdot 769\cdot 1489\cdot 2129\cdot 12641\cdot 25409\cdot 38321\cdot 191089\cdot 339161\cdot 1185601$	103
Lagrange Case 7 in Table 6.3	$2\cdot 79\cdot 7\cdot 13$	$41\cdot 353\cdot 1097\cdot 6089\cdot 10601\cdot 10993\cdot 24169\cdot 93481\cdot 252913\cdot 412081$	79, 7, 13
Theorem 4.1	$2\cdot 17\cdot 5\cdot 3\cdot 23\cdot 263\cdot 503$	$6857\cdot 11393\cdot 16553\cdot 53897\cdot 58337\cdot 68993\cdot 583673\cdot 868337$	17, 5, 3, 263, 503
None	$2\cdot 5\cdot 7\cdot 71\cdot 179\cdot 499$	$1201\cdot 1801\cdot 12401\cdot 13841\cdot 43649\cdot 57649\cdot 105449\cdot 290441\cdot 347729\cdot 1078841$	71, 179, 499

Notice that the value of β listed in the final row of Table 6.4 does not belong to a known family of non-congruent numbers. However, Monsky's formula can be used to verify that $s(2\cdot 5\cdot 7\cdot 71\cdot 179\cdot 499) = 0$, and so Theorem 6.1 can be applied to this value.

Table 6.5 lists a collection of non-congruent numbers that result from using Case I.2 of Theorem 6.1 to extend some of the non-congruent numbers described in Tables 4.1 and 6.3. Note that the first four numerical examples given in Table 6.5 also appear in Table 2 in [42]. These numbers have been included to illustrate how the non-congruent numbers generated by Case 1 of Theorem 1.1 in [42] are a subset of those produced by Case I.2 of Theorem 6.1.

Table 6.5: Non-congruent numbers $n = \beta s_{d+1} s_{d+2} \cdots s_t$ generated by Case I.2 of Theorem 6.1

Theorem Satisfied by β	$\boldsymbol{\beta}$	**Case I.2 Extension Tail $s_{d+1}s_{d+2}\cdots s_t$**	**Extension Tail Legendre Symbols that Equal −1**
Lagrange Case 6 in Table 6.3	$2{\cdot}79{\cdot}3{\cdot}13$	$73 \cdot 97 \cdot 313 \cdot 937 \cdot 1433 \cdot 1249 \cdot 10729 \cdot 12601{\cdot}19249{\cdot}17137$	$\left(\frac{73}{13}\right), \left(\frac{97}{13}\right), \left(\frac{313}{73}\right), \left(\frac{937}{79}\right), \left(\frac{1433}{3}\right), \left(\frac{1249}{1433}\right), \left(\frac{10729}{97}\right), \left(\frac{12601}{73}\right), \left(\frac{19249}{1433}\right), \left(\frac{17137}{19249}\right)$
Lagrange Case 6 in Table 6.3	$2 \cdot 23 \cdot 11 \cdot 13$	$113 \cdot 233 \cdot 257 \cdot 1049 \cdot 1193 \cdot 3433 \cdot 6337 \cdot 5641 \cdot 49201 \cdot 64793 \cdot 58217$	$\left(\frac{113}{23}\right), \left(\frac{233}{11}\right), \left(\frac{257}{233}\right), \left(\frac{1049}{23}\right), \left(\frac{1193}{23}\right), \left(\frac{3433}{113}\right), \left(\frac{6337}{13}\right), \left(\frac{5641}{6337}\right), \left(\frac{49201}{113}\right), \left(\frac{64793}{6337}\right), \left(\frac{58217}{64793}\right)$
Lagrange Case 6 in Table 6.3	$2 \cdot 103 \cdot 19 \cdot 5$	$17 \cdot 137 \cdot 409 \cdot 1721 \cdot 4409 \cdot 7681 \cdot 7753 \cdot 8209 \cdot 13001 \cdot 26449$	$\left(\frac{17}{5}\right), \left(\frac{137}{5}\right), \left(\frac{409}{19}\right), \left(\frac{1721}{103}\right), \left(\frac{4409}{17}\right), \left(\frac{7681}{17}\right), \left(\frac{7753}{5}\right), \left(\frac{8209}{409}\right), \left(\frac{13001}{409}\right), \left(\frac{26449}{17}\right)$
Lagrange Case 6 in Table 6.3	$2{\cdot}7{\cdot}11{\cdot}13$	$137 \cdot 257 \cdot 433 \cdot 641 \cdot 2129 \cdot 3697 \cdot 8969 \cdot 14561{\cdot}23761{\cdot}34057$	$\left(\frac{137}{13}\right), \left(\frac{257}{7}\right), \left(\frac{433}{7}\right), \left(\frac{641}{257}\right), \left(\frac{2129}{11}\right), \left(\frac{3697}{13}\right), \left(\frac{8969}{433}\right), \left(\frac{14561}{11}\right), \left(\frac{23761}{7}\right), \left(\frac{34057}{641}\right)$
Lagrange Case 1 in Table 6.3	$2 \cdot 3 \cdot 11$	$73 \cdot 313 \cdot 577 \cdot 97 \cdot 1433 \cdot 6689 \cdot 2689 \cdot 7297 \cdot 7129$	$\left(\frac{73}{11}\right), \left(\frac{313}{73}\right), \left(\frac{577}{73}\right), \left(\frac{97}{577}\right), \left(\frac{1433}{3}\right), \left(\frac{6689}{3}\right), \left(\frac{2689}{1433}\right), \left(\frac{7297}{1433}\right), \left(\frac{7129}{7297}\right)$
Theorem 4.1	$2 \cdot 41 \cdot 13 \cdot 19 \cdot 71 \cdot 31 \cdot 1319$	$617 \cdot 3769 \cdot 4001 \cdot 4937 \cdot 7673 \cdot 40897 \cdot 45161 \cdot 25913$	$\left(\frac{617}{13}\right), \left(\frac{3769}{41}\right), \left(\frac{4001}{41}\right), \left(\frac{4937}{41}\right), \left(\frac{7673}{41}\right), \left(\frac{40897}{4937}\right), \left(\frac{45161}{4001}\right), \left(\frac{25913}{71}\right)$

Next, we use Case II.3 of Theorem 6.1 to extend several non-congruent numbers β with $s(\beta) = 0$. For each of the first five examples listed in Table 6.6, β belongs to a known family of non-congruent numbers. For the remaining three examples, $s(\beta)$ can easily be shown to equal zero by forming the Monsky matrix corresponding to β and verifying that it has full rank. Also, note that the examples listed in the last two rows of Table 6.6 appear in Table 3 of [42]. This is because Case II.3.A of Theorem 6.1 generalizes Theorem 1.2 in [42].

Table 6.6: Non-congruent numbers $n = \beta s_{d+1} s_{d+2} \cdots s_t$ generated by Case II.3 of Theorem 6.1

Theorem Satisfied by β	$\boldsymbol{\beta}$	**Case II.3 Extension Tail $s_{d+1}s_{d+2}\cdots s_t$**	**Case(s) Satisfied by the Tail of Primes**
Lagrange Case 2 in Table 6.3	$2 \cdot 17 \cdot 5$	$3 \cdot 107 \cdot 347 \cdot 947 \cdot 1163 \cdot 3803 \cdot 11243 \cdot 12203 \cdot 22787 \cdot 31643 \cdot 373187 \cdot 562763$	Case II.3.B
Lagrange Case 2 in Table 6.3	$2 \cdot 17 \cdot 5$	$19 \cdot 251 \cdot 491 \cdot 1259 \cdot 1531 \cdot 6971 \cdot 3947 \cdot 44563 \cdot 115883 \cdot 304907 \cdot 662323 \cdot 1205123$	Case II.3.A (first six primes) and Case II.3.B (final six primes)
Lagrange Case 8 in Table 6.3	$2 \cdot 41 \cdot 47 \cdot 3$	$331 \cdot 1051 \cdot 1867 \cdot 3307 \cdot 3907 \cdot 4003 \cdot 25819 \cdot 59707 \cdot 72763 \cdot 110419$	Case II.3.D
Lagrange Case 8 in Table 6.3	$2 \cdot 41 \cdot 47 \cdot 3$	$107 \cdot 419 \cdot 443 \cdot 1091 \cdot 3499 \cdot 8803 \cdot 21211 \cdot 93139 \cdot 135043 \cdot 873043 \cdot 1217683 \cdot 1396987$	Case II.3.C (first four primes) and Case II.3.D (final eight primes)
Theorem 6.1 Case I.1	$2 \cdot 79 \cdot 7 \cdot 13 \cdot 41 \cdot 353$	$859 \cdot 1291 \cdot 8363 \cdot 22571 \cdot 58763 \cdot 76579 \cdot 215123 \cdot 325043 \cdot 326219 \cdot 890683$	Case II.3.C
None	$2 \cdot 5 \cdot 7 \cdot 71 \cdot 179 \cdot 499$	$1019 \cdot 19259 \cdot 40699 \cdot 55931 \cdot 130099 \cdot 180539 \cdot 239171 \cdot 313331$	Case II.3.A
None	$2 \cdot 41 \cdot 5 \cdot 31 \cdot 3$	$379 \cdot 3931 \cdot 3691 \cdot 5011 \cdot 10651 \cdot 32299$	Case II.3.A
None	$2 \cdot 73 \cdot 29 \cdot 47 \cdot 283$	$467 \cdot 971 \cdot 1531 \cdot 4003 \cdot 14243 \cdot 3467 \cdot 63691 \cdot 84299$	Case II.3.B (first two primes) and Case II.3.A (final six primes)

In Table 6.7, we state some non-congruent numbers that can be produced when Case III.3.A of Theorem 6.1 is used to extend non-congruent numbers either described by Lagrange's work, or listed in Tables 4.1, 6.5, or 6.6.

Table 6.7: Non-congruent numbers $n = \beta s_{d+1} s_{d+2} \cdots s_t$ generated by Case III.3.A of Theorem 6.1

Theorem Satisfied by β	$\boldsymbol{\beta}$	**Case III.3.A Extension Tail** $\boldsymbol{s_{d+1} s_{d+2} \cdots s_t}$
Lagrange Case 8 in Table 6.3	$2 \cdot 17 \cdot 7 \cdot 3$	$373 \cdot 421 \cdot 1381 \cdot 1429 \cdot 4813 \cdot 17077 \cdot 22453$
Lagrange Case 8 in Table 6.3	$2 \cdot 41 \cdot 23 \cdot 19$	$197 \cdot 821 \cdot 1373 \cdot 5717 \cdot 20149 \cdot 26573 \cdot 29741$
Theorem 4.1	$2 \cdot 17 \cdot 5 \cdot 3 \cdot 23 \cdot 263 \cdot 503$	$3109 \cdot 6949 \cdot 31741 \cdot 33469 \cdot 101149$
Theorem 4.1	$2 \cdot 41 \cdot 13 \cdot 19 \cdot 71 \cdot 31 \cdot 1319 \cdot 743 \cdot 3191$	$11701 \cdot 18773 \cdot 58733 \cdot 459749 \cdot 578213$
Theorem 6.1 Case I.2	$2 \cdot 79 \cdot 3 \cdot 13 \cdot 73 \cdot 97 \cdot 313$	$997 \cdot 3301 \cdot 12373 \cdot 20029 \cdot 42013$
Theorem 6.1 Case I.2	$2 \cdot 23 \cdot 11 \cdot 13 \cdot 113 \cdot 233 \cdot 257$	$653 \cdot 1013 \cdot 6653 \cdot 20333 \cdot 126949$
Theorem 6.1 Case I.2	$2 \cdot 103 \cdot 19 \cdot 5 \cdot 17 \cdot 137 \cdot 409$	$5381 \cdot 5861 \cdot 10429 \cdot 48109 \cdot 50261$
Theorem 6.1 Case I.2	$2 \cdot 7 \cdot 11 \cdot 13 \cdot 137 \cdot 257 \cdot 433$	$5581 \cdot 6029 \cdot 7253 \cdot 20549 \cdot 59557$
Theorem 6.1 Case II.3.A	$2 \cdot 41 \cdot 5 \cdot 31 \cdot 3 \cdot 379 \cdot 3931$	$3229 \cdot 9781 \cdot 26701 \cdot 27901 \cdot 28429 \cdot 74149$
Theorem 6.1 Case II.3.C	$2 \cdot 79 \cdot 7 \cdot 13 \cdot 41 \cdot 353 \cdot 859 \cdot 1291$	$1117 \cdot 12373 \cdot 30781 \cdot 51949 \cdot 129581 \cdot 225941 \cdot 678773$

It is also worthwhile to mention that the numbers described by Case (c) of Theorem 2 in Goto's paper [16] are a subset of those generated by Case III.3.A of Theorem 6.1. Goto's non-congruent numbers are a product of the integer two and arbitrarily many primes of the form $8k + 5$. His numbers follow the same pattern of Legendre symbols as the tail of primes of the form $8k + 5$ in Case III.3.A of Theorem 6.1.

Finally, in Table 6.8, we present some non-congruent numbers constructed according to Case IV.4 of Theorem 6.1.

Table 6.8: Non-congruent numbers $n = \beta s_{d+1} s_{d+2} \cdots s_t$ generated by Case IV.4 of Theorem 6.1

Theorem Satisfied by $\boldsymbol{\beta}$	$\boldsymbol{\beta}$	**Case IV.4 Extension Tail $\boldsymbol{s_{d+1}s_{d+2}\cdots s_t}$**	**Element(s) in $\boldsymbol{H}$**
Lagrange Case 4 in Table 6.3	$2 \cdot 73 \cdot 3 \cdot 11$	$359 \cdot 167 \cdot 1823 \cdot 6599 \cdot 2063 \cdot 20327 \cdot 20063 \cdot 85439 \cdot 431903 \cdot 138959$	73
Lagrange Case 4 in Table 6.3	$2 \cdot 73 \cdot 3 \cdot 11$	$479 \cdot 79 \cdot 359 \cdot 5623 \cdot 6863 \cdot 8887 \cdot 8087 \cdot 77743 \cdot 38543 \cdot 98911$	3
Lagrange Case 4 in Table 6.3	$2 \cdot 73 \cdot 3 \cdot 11$	$503 \cdot 31 \cdot 1487 \cdot 823 \cdot 10247 \cdot 4519 \cdot 70583 \cdot 65839 \cdot 278879 \cdot 218887 \cdot 541439 \cdot 268063$	73, 3, 11
Lagrange Case 5 in Table 6.3	$2 \cdot 17 \cdot 13 \cdot 29$	$103 \cdot 127 \cdot 1223 \cdot 599 \cdot 10039 \cdot 5087 \cdot 26399 \cdot 9103 \cdot 253751 \cdot 108359$	29
Lagrange Case 5 in Table 6.3	$2 \cdot 17 \cdot 13 \cdot 29$	$919 \cdot 239 \cdot 1223 \cdot 463 \cdot 5407 \cdot 1879 \cdot 18199 \cdot 3583 \cdot 200983 \cdot 68543$	13
Lagrange Case 5 in Table 6.3	$2 \cdot 17 \cdot 13 \cdot 29$	$647 \cdot 23 \cdot 103 \cdot 199 \cdot 4943 \cdot 14303 \cdot 38047 \cdot 16007 \cdot 430847 \cdot 104623$	17
Theorem 6.1 Case III.3.A	$2 \cdot 79 \cdot 7 \cdot 13 \cdot 41 \cdot 353 \cdot 859 \cdot 1291 \cdot 1117$	$2287 \cdot 239 \cdot 207847 \cdot 74687 \cdot 392831 \cdot 275039 \cdot 650543 \cdot 2165039$	79, 7, 13, 41, 353
Theorem 6.1 Case III.3.A	$2 \cdot 79 \cdot 7 \cdot 13 \cdot 41 \cdot 353 \cdot 859 \cdot 1291 \cdot 1117$	$14551 \cdot 12959 \cdot 161503 \cdot 142543 \cdot 986543 \cdot 594119 \cdot 1492063 \cdot 3703823$	7, 13, 41, 353, 859, 1291, 1117
Theorem 6.1 Case III.3.A	$2 \cdot 79 \cdot 7 \cdot 13 \cdot 41 \cdot 353 \cdot 859 \cdot 1291 \cdot 1117$	$2287 \cdot 607 \cdot 27583 \cdot 60623 \cdot 298847 \cdot 401743$	1117

Note that it is possible to combine the cases in Theorem 6.1 to produce even non-congruent numbers with prime factors in each odd congruence class modulo eight. The numerical examples in the final three rows of Table 6.8 are generated by applying Cases I.1, II.3.C, III.3.A, and IV.4 of Theorem 6.1 to a non-congruent number described by Lagrange [27].

Chapter 7

Conclusion

This thesis focused on the generation of non-congruent numbers with arbitrarily many distinct prime divisors. Our results are significant because they provide a new technique for constructing non-congruent numbers, and produce families of both odd and even non-congruent numbers containing prime factors belonging to each odd congruence class modulo eight. We begin by summarizing our main research contributions and then proceed to discuss some interesting avenues for future work.

7.1 Main Results

In Chapter 4, we described a particular family of even non-congruent numbers that are a product of arbitrarily many primes. These non-congruent numbers have at least one prime factor in each odd congruence class modulo eight. This is a distinguishing feature of our result, as all known families of even non-congruent numbers are comprised of primes belonging to no more than three odd congruence classes modulo eight.

Chapters 5 and 6 developed and described a general approach for constructing non-congruent numbers. Our method allows any non-congruent number α, for which the elliptic curve $y^2 = x^3 - \alpha^2 x$ has 2-Selmer rank equal to zero, to be extended to produce other non-congruent numbers. Chapter 5 focused on odd non-congruent numbers, and showed that infinitely many non-congruent numbers can be generated by appending arbitrarily many primes of the form $8k+1$, $8k+3$, or $8k+5$ onto known odd non-congruent numbers. In Chapter 6, we considered even non-congruent numbers and provided criteria for constructing non-congruent numbers with arbitrarily many prime factors in possibly all of the four odd congruence classes modulo eight. Our results in Chapters 5 and 6 allow existing families of non-congruent numbers to be extended and thus, considerably broaden the collection of non-congruent numbers that can be generated and described.

7.2 Future Work

In this section, we identify and discuss some directions for future research work.

1) Theorem 5.5 produces an infinite collection of non-congruent numbers by multiplying existing odd non-congruent numbers α with $s(\alpha) = 0$ by primes $s_{d+1}, s_{d+2}, \ldots, s_t$ of the form $8k + 1$, $8k + 3$, or $8k + 5$. Is it possible to find primes $s_{d+1}, s_{d+2}, \ldots, s_t$ of the form $8k + 7$ with t even, such that for any odd number α with $s(\alpha) = 0$, the integer $n = \alpha s_{d+1} s_{d+2} \cdots s_t$ is a non-congruent number with $s(n) = 0$?

2) It would be interesting to determine whether Theorems 5.5 and 6.1 can be expanded to describe a larger collection of non-congruent numbers. In Theorem 5.5, the primes $s_{d+1}, s_{d+2}, \ldots, s_t$ that are appended onto the odd non-congruent number α are required to satisfy specific Legendre symbol conditions. Do there exist Legendre symbol conditions that differ from those in the statement of Theorem 5.5 that, when imposed upon the primes $s_{d+1}, s_{d+2}, \ldots, s_t$, guarantee that $\alpha s_{d+1} s_{d+2} \cdots s_t$ is a non-congruent number with $s(\alpha) = 0$? Similarly, are there Legendre symbol conditions other than the ones stated in Theorem 6.1 that allow the even non-congruent number β with $s(\beta) = 0$ to be extended to produce infinitely many non-congruent numbers $\beta s_{d+1} s_{d+2} \cdots s_t$? Furthermore, if Theorems 5.5 and 6.1 can be expanded, is there a better, more concise way to describe all of the Legendre symbol conditions?

3) There exist non-congruent numbers whose corresponding congruent number elliptic curves have nonzero 2-Selmer rank. For example, Bastien [2] described a family of non-congruent numbers of the form $n = 2p$ with $p \equiv 9 \pmod{16}$ for which $s(n) > 0$. Congruent number elliptic curves with rank equal to zero and non-trivial Shafarevich-Tate group are also given by Wang [58]; the non-congruent numbers that he describes have arbitrarily many prime divisors. It would be desirable to find other families of non-congruent numbers with nonzero 2-Selmer rank.

4) The work in this thesis strictly focused on the construction of non-congruent numbers with arbitrarily many prime factors. However, it would be of interest to find families of congruent numbers with arbitrarily many prime divisors. Families of congruent numbers with two or fewer odd prime factors were given by Heegner [21], Birch [4],

Stephens [53], and Monsky [34]. More recently Tian described some families of congruent numbers that have an unlimited number of prime divisors [7, 54, 55]. Because the 2-Selmer rank provides an upper bound for the arithmetic rank, Monsky's formula for computing the 2-Selmer rank of E_n cannot be used in isolation to generate families of congruent numbers. This makes the search for families of congruent numbers with arbitrarily many distinct prime factors a substantially more challenging task than the search for families of non-congruent numbers of a similar form.

5) Monsky's formula, which is described in Section 3.6, computes the 2-Selmer rank of congruent number elliptic curves $y^2 = x^3 - n^2x$. A natural extension would be to examine whether or not it is possible to use Monsky's approach to calculate the 2-Selmer rank of other elliptic curves. In [17], Goto studies a more general version of the congruent number problem, known as the θ-congruent number problem. This involves determining whether a positive integer is a θ-congruent number. A positive integer n is called a θ-congruent number if $n\sqrt{r^2 - s^2}$ occurs as the area of a triangle with rational side lengths and an angle $0 < \theta < \pi$, where $\cos(\theta) = s/r$ with $s, r \in \mathbb{Z}$, $|s| \leq r$, and $(r, s) = 1$. The θ-numbers are related to elliptic curves of the form

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

Note that $\pi/2$-congruent numbers are regular congruent numbers. Goto claims that he "could not apply Monsky's method to the θ-congruent number problem with $\theta \neq \pi/2$". However, he does not provide any further details regarding this, and so it is unclear whether it is in fact impossible to derive a formula for computing the 2-Selmer rank of elliptic curves for θ-congruent numbers with $\theta \neq \pi/2$.

Bibliography

[1] R. Alter, T. B. Curtz, and K. K. Kubota, *Remarks and results on congruent numbers*, Proc. Third Southeastern Conf. on Combinatorics, Graph Theory and Computing, (1972), pp. 27–35. → pages 24

[2] L. Bastien, *Nombres congruents*, Intermédiaire des Math., 22 (1915), pp. 231–232. → pages 4, 31, 46, 72, 101, 109

[3] M. Bhargava and A. Shankar, *Ternary cubic forms having bounded invariants, and the existence of a positive proportion of elliptic curves having rank 0*, Ann. of Math. (2), 181 (2015), pp. 587–621. → pages 24

[4] B. J. Birch, *Elliptic curves and modular functions*, in Symposia Mathematica, Indam Rome 1968/1969, Vol. 4, Academic Press, 1970, pp. 27–32. → pages 109

[5] V. Chandrasekar, *The congruent number problem*, Resonance, 3 (1998), pp. 33–45. → pages 2, 3, 26

[6] W. Cheng and X. Guo, *Some new families of non-congruent numbers*, J. Number Theory, 196 (2019), pp. 291–305. → pages 4, 31, 46, 72, 101

[7] J. Coates, *Congruent numbers*, Acta Math. Vietnam, 39 (2014), pp. 3–10. → pages 25, 110

[8] L. E. Dickson, *History of the Theory of Numbers, II*, Carnegie Institution of Washington, Washington, 1920. → pages 2, 3

[9] A. Dujella, *History of elliptic curves rank records.* `https://web.math.pmf.unizg.hr/~duje/tors/rankhist.html`. Accessed: 2019-07-13. → pages 24

[10] A. Dujella, A. S. Janfada, and S. Salami, *A search for high rank congruent number elliptic curves*, J. Integer Seq., 12 (2009). Article 09.5.8. → pages 24, 25, 26, 29

[11] K. Feng, *Non-congruent numbers, odd graphs and the Birch-Swinnerton-Dyer conjecture*, Acta Arith., 75 (1996), pp. 71–83. → pages 4, 31, 46, 72, 101

[12] K. Feng and M. Xiong, *On elliptic curves $y^2 = x^3 - n^2x$ with rank zero*, J. Number Theory, 109 (2004), pp. 1–26. → pages 31, 101

[13] K. Feng and Y. Xue, *New series of odd non-congruent numbers*, Sci. China Ser. A, 49 (2006), pp. 1642–1654. → pages 4, 31, 46, 72

[14] J. B. Fraleigh, *A First Course in Abstract Algebra*, Addison Wesley, Boston, seventh ed., 2003. → pages 5

[15] A. Genocchi, *Note analitiche sopra tre scritti*, Annali di Scienze Matematiche e Fisiche, 6 (1855), pp. 273–317. → pages 4, 31, 46, 72, 101

[16] T. Goto, *A note on the Selmer group of the elliptic curve $y^2 = x^3+Dx$*, Proc. Japan Acad. Ser. A Math. Sci., 77 (2001), pp. 122–125. → pages 31, 106

[17] ——, *A Study on the Selmer Groups of Elliptic Curves with a Rational 2-Torsion*, PhD thesis, Kyushu University, 2002. → pages 4, 46, 72, 73, 101, 102, 110

[18] F. Q. Gouvêa, *p-adic Numbers: An Introduction*, Springer-Verlag, New York, second ed., 1997. → pages 9, 10

[19] D. R. Heath-Brown, *The size of Selmer groups for the congruent number problem*, Invent. Math., 111 (1993), pp. 171–195. → pages 29

[20] ——, *The size of Selmer groups for the congruent number problem, II. With an appendix by P. Monsky*, Invent. Math., 118 (1994), pp. 331–370. → pages 29, 30

[21] K. Heegner, *Diophantische analysis und modulfunktionen*, Math Z., 56 (1952), pp. 227–253. → pages 109

[22] B. Hemenway, *On Recognizing Congruent Primes*, Master's thesis, Simon Fraser University, 2006. → pages 21

[23] D. Husemöller, *Elliptic Curves, Graduate Texts in Mathematics, 111*, Springer-Verlag, New York, second ed., 2004. → pages 12, 14, 15, 16, 18, 19, 20, 29

[24] B. Iskra, *Non-congruent numbers with arbitrarily many prime factors congruent to 3 modulo 8*, Proc. Japan Acad. Ser. A Math. Sci., 72 (1996), pp. 168–169. → pages 4, 27, 31, 46, 72

[25] N. Koblitz, *Introduction to Elliptic Curves and Modular Forms, Graduate Texts in Mathematics, 97*, Springer-Verlag, New York, second ed., 1993. → pages 2, 3, 12, 18, 21

[26] J. H. Kwak and S. Hong, *Linear Algebra*, Springer, New York, second ed., 2004. → pages 10

[27] J. Lagrange, *Nombres congruents et courbes elliptiques*, Séminaire Delange-Pisot-Poitou, Théorie des nombres, 16e année (1974/1975). → pages 4, 25, 31, 46, 72, 73, 101, 107

[28] D. Li and Y. Tian, *On the Birch-Swinnerton-Dyer conjecture of elliptic curves $E_D : y^2 = x^3 - D^2x$*, Acta Math. Sin. (Engl. Ser.), 16 (2000), pp. 229–236. → pages 4, 31, 46, 72

[29] A. Lonzano-Robledo, *Elliptic Curves, Modular Forms, and Their L-functions (Student Mathematical Library)*, American Mathematical Society, 2011. → pages 2, 15, 18, 19, 20, 28, 29

[30] B. Mazur, *Modular curves and the Eisenstein ideal*, Inst. Hautes Études Sci. Publ. Math., 47 (1977), pp. 33–186. → pages 21

[31] ——, *Rational isogenies of prime degree*, Invent. Math., 44 (1978), pp. 129–162. → pages 20, 21

[32] R. B. McClenon, *Leonardo of Pisa and his Liber Quadratorum*, Amer. Math. Monthly, 26 (1919), pp. 1–8. → pages 2

[33] C. D. Meyer, *Matrix Analysis and Applied Linear Algebra*, SIAM, Philadelphia, 2000. → pages 10, 11

[34] P. Monsky, *Mock Heegner points and congruent numbers*, Math. Z., 204 (1990), pp. 45–67. → pages 25, 110

[35] K. Noda and H. Wada, *All congruent numbers less than 10000*, Proc. Japan Acad. Ser. A Math. Sci., 69 (1993), pp. 175–178. → pages 2

[36] Y. Ouyang and S. Zhang, *On non-congruent numbers with 1 modulo 4 prime factors*, Sci. China Math., 57 (2014), pp. 649–658. → pages 4, 31, 46, 72

[37] ——, *On second 2-descent and non-congruent numbers*, Acta Arith., 170 (2015), pp. 343–360. → pages 4, 31, 46, 72, 101

[38] L. Reinholz, *Families of Congruent and Non-congruent Numbers*, Master's thesis, The University of British Columbia, 2013. → pages 27, 46

[39] L. Reinholz, B. K. Spearman, and Q. Yang, *Families of non-congruent numbers with arbitrarily many prime factors*, J. Number Theory, 133 (2013), pp. 318–327. → pages 4, 31, 46, 72

[40] ——, *On the prime factors of non-congruent numbers*, Colloq. Math., 138 (2015), pp. 271–282. → pages 4, 31, 46, 72, 75, 76

[41] ——, *An extension theorem for generating new families of non-congruent numbers*, Funct. Approx. Comment. Math., 58 (2018), pp. 69–77. → pages v, 41, 42

[42] ——, *Families of even non-congruent numbers with prime factors in each odd congruence class modulo eight*, Int. J. Number Theory, 14 (2018), pp. 669–692. → pages v, vi, 31, 80, 85, 86, 103, 104

[43] L. Reinholz and Q. Yang, *On the extension of even families of non-congruent numbers*. Submitted for publication. → pages v, vi, 80

[44] ——, *On the generation of odd non-congruent numbers with arbitrarily many prime factors*. Submitted for publication. → pages v, 41, 48

[45] N. Rogers, *Elliptic curves $x^3 + y^3 = k$ with high rank*, PhD thesis, Harvard University, 2004. → pages 24

[46] K. H. Rosen, *Elementary Number Theory and its Applications*, Addison Wesley, Boston, fifth ed., 2005. → pages 2, 6, 7, 8, 9

[47] S. Schmitt and H. G. Zimmer, *Elliptic Curves: A Computational Approach*, Walter de Gruyter, Berlin, 2003. → pages 12, 15, 16

[48] E. S. Selmer, *The Diophantine equation $ax^3 + by^3 + cz^3 = 0$*, Acta Math., 85 (1951), pp. 203–362. → pages 10

[49] P. Serf, *Congruent numbers and elliptic curves*, in Computational Number Theory, A. Pethö, M. E. Pohst, H. C. Williams, and H. G. Zimmer, eds., Walter de Gruyter, 1991, pp. 227–238. → pages 4, 25, 26, 28, 31, 46, 72, 101

[50] J. P. Serre, *A Course in Arithmetic, Graduate Texts in Mathematics, 7*, Springer-Verlag, New York, 1973. → pages 9, 10

[51] J. H. Silverman, *The Arithmetic of Elliptic Curves, Graduate Texts in Mathematics, 106*, Springer, New York, second ed., 2009. → pages 12, 13, 15, 16, 18, 19, 20, 24, 26, 28, 29

[52] J. H. Silverman and J. T. Tate, *Rational Points on Elliptic Curves, Undergraduate Texts in Mathematics*, Springer, New York, second ed., 2015. → pages 12, 13, 15, 16, 18, 19, 20

[53] N. M. Stephens, *Congruence properties of congruent numbers*, Bull. London Math. Soc., 7 (1975), pp. 182–184. → pages 110

[54] Y. Tian, *Congruent numbers with many prime factors*, Proc. Natl. Acad. Sci. USA, 109 (2012), pp. 21256–21258. → pages 25, 110

[55] ——, *Congruent numbers and Heegner points*, Camb. J. Math., 2 (2014), pp. 117–161. → pages 25, 110

[56] J. Top and N. Yui, *Congruent number problems and their variants*, Algorithmic number theory: lattices, number felds, curves and cryptography, 44 (2008), pp. 613–639. → pages 2, 3

[57] J. B. Tunnell, *A classical Diophantine problem and modular forms of weight 3/2*, Invent. Math., 72 (1983), pp. 323–334. → pages 2, 3

[58] Z. Wang, *Congruent elliptic curves with non-trivial Shafarevich-Tate groups*, Sci. China Math., 59 (2016), pp. 2145–2166. → pages 4, 31, 46, 72, 109

[59] L. C. Washington, *Elliptic Curves: Number Theory and Cryptography*, Chapman and Hall/CRC, New York, 2003. → pages 18, 19, 20

[60] A. Wiles, *The Birch and Swinnerton-Dyer Conjecture*, 2000. `http://www.claymath.org/sites/default/files/birchswin.pdf`. → pages 2, 3

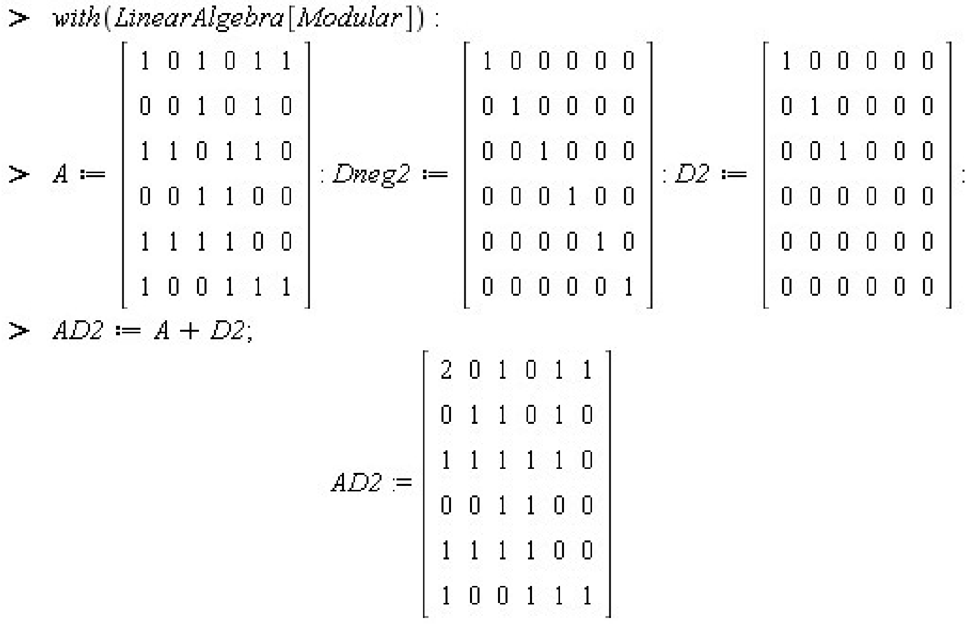
Appendix

Appendix A

Maple & Magma Code

In Sections 4.3, 5.3, 5.5, and 6.3, we presented numerical examples generated by our main theorems. In this section, we show how to use Maple to construct those numbers as well as infinitely many other non-congruent numbers satisfying the constraints imposed in the statements of our theorems in Chapters 4, 5, and 6.

We illustrate the process by considering the non-congruent number $n = (\alpha)s_1s_2\cdots s_8 = (13\cdot 29\cdot 37\cdot 23\cdot 31\cdot 71)\cdot 4003\cdot 5867\cdot 41947\cdot 60779\cdot 135131\cdot 196387\cdot 296299\cdot 329891$ listed in Table 5.5. Since α does not belong to a known family of non-congruent numbers, we begin by verifying that $\alpha = (13\cdot 29\cdot 37\cdot 23\cdot 31\cdot 71)$ satisfies $s(\alpha) = 0$. We do this by using Monsky's formula, given by Equation (3.15). The following code shows how Maple is used to compute the rank of the Monsky matrix, $\mathbf{M_o}$, for α. Note that in the code, the diagonal matrices $\mathbf{D_{-2}}$ and $\mathbf{D_2}$ are denoted by *Dneg2* and *D2*, respectively.

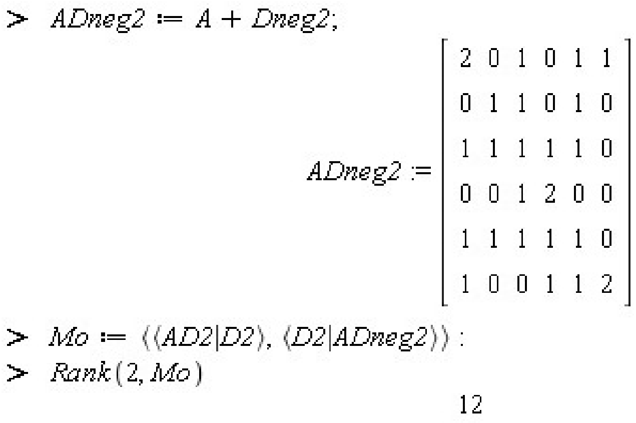


```
> with(LinearAlgebra[Modular]):
```

$$> A := \begin{bmatrix} 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 1 \end{bmatrix} : Dneg2 := \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix} : D2 := \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix} :$$

```
> AD2 := A + D2;
```

$$AD2 := \begin{bmatrix} 2 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 1 \end{bmatrix}$$

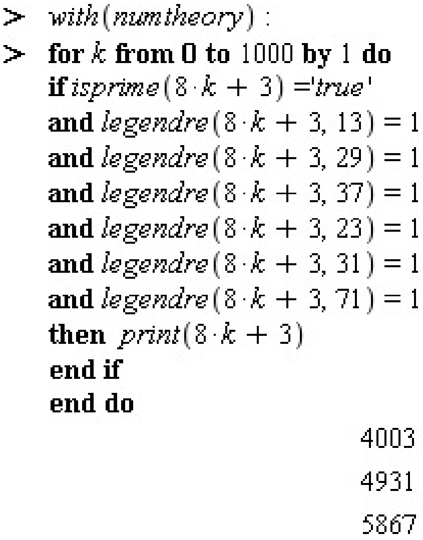


```
> ADneg2 := A + Dneg2;
                         [2 0 1 0 1 1]
                         [0 1 1 0 1 0]
                         [1 1 1 1 1 0]
              ADneg2 :=  [0 0 1 2 0 0]
                         [1 1 1 1 1 0]
                         [1 0 0 1 1 2]
> Mo := ⟨⟨AD2|D2⟩, ⟨D2|ADneg2⟩⟩ :
> Rank(2, Mo)
                              12
```

Since $\text{rank}_{\mathbb{F}_2}(\mathbf{M_o}) = 12$, Equation (3.15) implies that $s(\alpha) = 0$, as required.

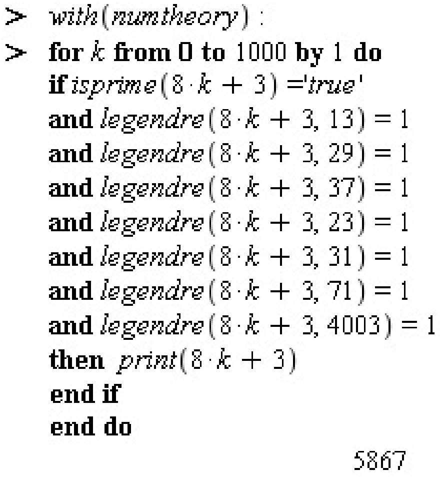
If α is even, an analogous set of Maple calculations can be completed to determine the rank of the matrix $\mathbf{M_e}$, given by Equation (3.17).

Our next step is to generate new non-congruent numbers by finding a tail of primes to append onto α that satisfy the Legendre symbol conditions specified in the statement of Theorem 5.5 Case I.1.A. This can be done efficiently by using the following Maple code.



```
> with(numtheory) :
> for k from 0 to 1000 by 1 do
  if isprime(8·k + 3) ='true'
  and legendre(8·k + 3, 13) = 1
  and legendre(8·k + 3, 29) = 1
  and legendre(8·k + 3, 37) = 1
  and legendre(8·k + 3, 23) = 1
  and legendre(8·k + 3, 31) = 1
  and legendre(8·k + 3, 71) = 1
  then print(8·k + 3)
  end if
  end do
                    4003
                    4931
                    5867
```

Notice that in this loop, the six required Legendre symbol conditions are specified and primes of the form $8k + 3$ satisfying the conditions are listed in the output. For k values from 0 to 1000, three primes are stated in the output. We choose to append the first prime listed, 4003, onto α. We then update the Legendre symbol conditions to include the condition imposed on the prime 4003, and run the code again to find another prime to append onto $\alpha \cdot 4003$. Our search yields the prime 5867, as shown by the following code.



```
> with(numtheory) :
> for k from 0 to 1000 by 1 do
  if isprime(8·k + 3) ='true'
  and legendre(8·k + 3, 13) = 1
  and legendre(8·k + 3, 29) = 1
  and legendre(8·k + 3, 37) = 1
  and legendre(8·k + 3, 23) = 1
  and legendre(8·k + 3, 31) = 1
  and legendre(8·k + 3, 71) = 1
  and legendre(8·k + 3, 4003) = 1
  then print(8·k + 3)
  end if
  end do
                                5867
```

This process can be repeated indefinitely, allowing arbitrarily many primes of the form $8k+3$ to be appended onto α, and infinitely many non-congruent numbers to be produced. Note that if the code fails to return an output, then the bounds for k need to be adjusted.

The numbers generated by our theorems can be verified to be non-congruent by using the computer algebra system Magma. This is found online at

`http://magma.maths.usyd.edu.au/calc/`.

The code below shows how Magma is used to calculate the Mordell-Weil rank of the congruent number elliptic curve corresponding to the integer $\alpha s_1 = (13 \cdot 29 \cdot 37 \cdot 23 \cdot 31 \cdot 71) \cdot 4003$.

Input:

```
E:=EllipticCurve([-(13*29*37*23*31*71*4003)^2,0]);
Rank(E);
```

Output:

```
0 true
```

Magma confirms that the rank of the curve $y^2 = x(x^2 - (\alpha s_1)^2)$ is zero, so $\alpha s_1 = (13 \cdot 29 \cdot 37 \cdot 23 \cdot 31 \cdot 71) \cdot 4003$ is a non-congruent number.