Congruent Numbers and Elliptic Curves

by

Jennifer Ann Johnstone

B.Sc. Hons., The University of British Columbia, 2009

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

MASTER OF SCIENCE

in

The College of Graduate Studies

(Mathematics)

THE UNIVERSITY OF BRITISH COLUMBIA

(Okanagan)

July 2010

Abstract

Throughout this thesis we will be primarily concerned with the area of a rational right angle triangle, also known as a congruent number. The purpose of this thesis is to present a family of congruent number elliptic curves with rank at least three, as well as provide some insight into the distribution of congruent numbers. We provide an in depth background on congruent numbers and elliptic curves, as well as an overview of one of the key methods that will be used in determining the rank of an elliptic curve.

Table of Contents

Appendices

List of Figures

List of Notation

$\mathbb{Z}$	Set of integers $\{\ldots,-2,-1,0,1,2,\ldots\}$	2.
$a \equiv b (\bmod m)$	Congruent	3.
$\gcd(a,b)$	Greatest common divisor	5.
$a \mid b$	Divides	5.
$a \nmid b$	Does not divide	5.
$p^a \parallel n$	Exactly divides	5.
$\prod$	Product	6.
$\mathbb{Z}^+$	Set of positive integers $\{1,2,3,\ldots\}$	7.
$\mathbb{Q}$	Set of rational numbers	7.
$E(\mathbb{Q})$	Set of rational points on an elliptic curve	19.
$\mathcal{O}$	Point at infinity on an elliptic curve	20.
$\mathbb{Q}^*$	Set of non-zero rational numbers	24.
$\mathbb{Q}^{*2}$	Set of squares of non-zero rational numbers	24.
$\frac{\mathbb{Q}^*}{\mathbb{Q}^{*2}}$	Quotient group	24.

Acknowledgements

To start, the author would like to express her deepest gratitude to her supervisor Dr. Blair Spearman for his constant support and guidance throughout this process. The ideas presented in this thesis are the result of two summers of research with Dr. Spearman, which would not have been possible without the support of the Natural Sciences and Engineering Research Council of Canada.

The author would also like to thank her committee Dr. Qiduan Yang and Dr. Yves Lucet for their helpful suggestions and all of the time they devoted to this success.

Finally, the author would also like to acknowledge and thank all of the people who encouraged her to complete her Masters and supported her throughout.

Dedication

To my mother.

Chapter 1

Introduction

Although there are several equivalent definitions, the best way to define a congruent number is to first recall a similar, well known, property involving pythagorean triples. *Pythagorean triples* are defined as triples of positive integers satisfying the equation $x^2 + y^2 = z^2$, such that each triple forms a right angle triangle with integer sides. Specifically, x, y and z can be defined to generate all possible pythagorean triples [Ros05]. This in turn allows us to find all possible integers m that will produce a right angle triangle with integer sides [Ros05].

To turn this to the definition of a congruent number we need to consider the possible integers n that will result in a right angle triangle with rational sides. That is to say, congruent numbers are defined as follows.

Definition 1.1. A positive integer n is a *congruent number* if there exists a rational right angle triangle with area n.

For example, 6 is a congruent number since there exists a rational right angle triangle with area 6, namely the right angle triangle seen in Figure 1.1.

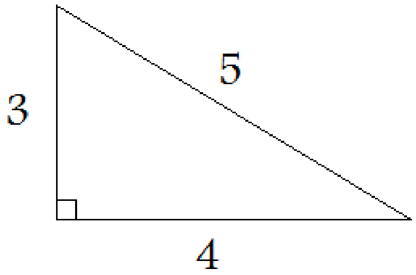

Figure 1.1: Rational right angle triangle with area 6.

Notably, congruent numbers were first documented in a 10th century Arab manuscript and have since been studied by numerous scholars, including Euler, Fibonacci, and Fermat [AC74, Alt80, Kra86, Coa05, Cip09, Cha06, Hem06, Tun83]. In 1225 Fibonacci was the first to show that 5 and 7 are congruent numbers [Cha06]. Fibonacci also stated, without proof, that no congruent number n is exactly a square [Cha98]. It was not until four centuries later that Fermat proved Fibonacci's statement, using the method of infinite descent. Specifically, Fermat proved that 1 is not a congruent number [Cha98, DJS09, Coa05, Cip09, Cha06].

When discussing congruent numbers we are often interested in the *congruent number problem*, which is as follows.

Given a positive integer n *can we determine whether or not* n *is a congruent number in a finite number of steps? [Cha98, Coa05, Hem06]*

Since the 10th century many different definitions of congruent numbers have been derived in order to try and solve the congruent number problem. However, unlike right angle triangles with integer sides the congruent number problem remains unsolved [Cha98].

Even though congruent numbers in general have been around for a very long time, and lots of work has gone into finding them, it took until 1915 to list all congruent numbers less than 100. This in turn led to another goal "Finding all square-free congruent numbers less than 1000" [Alt80, AC74, Cip09]. It was not until 1983 when Tunnell determined an equivalent definition for a congruent number that ultimately allowed for all congruent numbers less than 1000 to be determined [Cip09, Hem06]. Tunnell also provided a simple criterion to determine whether or not a positive integer n is a congruent number [Hem06, Ros05].

Theorem 1.2. [Hem06, Ros05, Kob92, Tunnell's Theorem] *Define*

$$\begin{aligned} A_n &= \#\left\{x,y,z\in\mathbb{Z}|n=2x^2+y^2+32z^2\right\} \\ B_n &= \#\left\{x,y,z\in\mathbb{Z}|n=2x^2+y^2+8z^2\right\} \\ C_n &= \#\left\{x,y,z\in\mathbb{Z}|n=4x^2+2y^2+64z^2\right\} \\ D_n &= \#\left\{x,y,z\in\mathbb{Z}|n=8x^2+2y^2+16z^2\right\}. \end{aligned}$$

Suppose n is congruent, if n is even then

$$A_n = B_n$$

and if n is odd, then

$$2C_n = D_n.$$

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

Proof. See [Kob92] for the logical structure of the argument.

□

As we can see the converse of Tunnell's Theorem hinges on the BSD Conjecture, which is still an open problem today. Details about the BSD Conjecture are, however, beyond the scope of this thesis. Fortunately, the results found in this thesis do not assume the BSD Conjecture, but it is worth mentioning that the BSD Conjecture is one of the Clay Mathematics Institutes Millennium Prize Problems and it is widely assumed to be true [Hem06, Cip09].

Since 1983 a lot more work has been done to determine congruent numbers, including some results that do not use Tunnell's Theorem. In 1986 Kramarz verified the converse of Tunnell's Theorem for all square-free integers less than 2000 [Kra86]. By 1993, with the help of computers and the use of Tunnell's Theorem, all congruent numbers less than 10000 had been determined [NW93]. Today's results include computations for congruent numbers up to 1 trillion, once again assuming Tunnell's Theorem [Cip09].

Currently, Rubinstein and others have predicted that the number of congruent numbers less than x, arising from even rank elliptic curves, is asymptotically

$$cx^{3/4}\log(x)^{11/8}, \tag{1.1}$$

where c is a constant. It is their hope to provide a better determination of c, using the data produced from the computations for congruent numbers up to 1 trillion [Cip09].

We now provide some of the other known results that do not assume the BSD Conjecture. For instance, given distinct primes p_i and q_i where $p_i \equiv q_i \equiv i \pmod 8$, i.e. $p_i = 8k + i$ and $q_i = 8l + i$ for some $k, l \in \mathbb{Z}$, we have the following results, as stated in [Hem06, Tun83].

1. p_3 is not a congruent number.

2. $p_3q_3, 2p_5, 2p_5q_5$ are not congruent numbers.

3. p_5, p_7 are congruent numbers.

4. $2p_7, 2p_3, p_3q_7, 2p_3q_5, 2p_5q_7$ are congruent numbers.

One of the main results, to be presented in Chapter 5, is that we were able to find a family of congruent numbers, for which the associated elliptic curve satisfies a rank condition. These results have been accepted for publication in the Canadian Mathematical Bulletin under the title "Congruent Number

Elliptic Curves with rank at least Three". Another main result, to be presented in Chapter 6, involves the distribution of congruent numbers and has been recently published in the Proceedings of the Japan Academy, Series A, under the title "On the Distribution of Congruent Numbers". Before we present these results we will provide the necessary background information in the next section followed by an in depth chapter on congruent numbers. In Chapter 3 we provide the necessary definitions and theorems for elliptic curves followed by a discussion on how to calculate the rank of an elliptic curve in Chapter 4.

1.1 Preliminaries

To start, we recall some basics from Abstract Algebra that can be found in most first year Abstract Algebra textbooks. We begin with some definitions involving *binary algebraic structures*, denoted by $< G, * >$, where G is a set and $*$ is a binary operator.

Definition 1.3. A *group* $< G, * >$ is a set G, closed under a binary operation $*$, such that

1. $(a*b)*c = a*(b*c)$ for all $a, b, c \in G$ (i.e. $*$ is associative with respect to G).

2. $e * a = a * e = a$ for all $a \in G$ and some element $e \in G$ (i.e. there exists an identity element e in G for $*$).

3. Corresponding to each $a \in G$, there is an element $a' \in G$ such that $a * a' = a' * a = e$ (i.e. G contains inverses with respect to $*$).

Definition 1.4. An *abelian group* $< G, * >$ is a group G where $a * b = b * a$ for all $a, b \in G$ (i.e. $*$ is commutative).

Definition 1.5. Let $< G, * >$ and $< G', *' >$ be binary algebraic structures, where G and G' are both groups. Then a map ϕ of G into G' is a *homomorphism* if

$$\phi(a * b) = \phi(a) *' \phi(b)$$

for all $a, b \in G$.

Definition 1.6. Let $< G, * >$ and $< G', *' >$ be binary algebraic structures. An *isomorphism* of G with G', denoted by $G \simeq G'$, is a one-to-one function ϕ mapping G onto G' such that

$$\phi(a * b) = \phi(a) *' \phi(b)$$

for all $a, b \in G$.

We also define a *generator* for a group $< G, * >$ as an element $a \in G$ that generates G under the assumed binary operation $*$ (i.e. if $G = \{a^n | n \in \mathbb{Z}\}$ for some a in G then we say that a is a generator for G). Lastly, we define finitely generated abelian groups and recall the Fundamental Theorem of Finitely Generated Abelian Groups, as follows.

Definition 1.7. A *finitely generated abelian group* $< G, * >$ is an abelian group that contains a finite set of generators of G.

Theorem 1.8. [Fra03, Fundamental Theorem of Finitely Generated Abelian Groups] *Every finitely generated abelian group G is isomorphic to a direct sum of cyclic groups in the form*

$$\mathbb{Z} \bigoplus \cdots \bigoplus \mathbb{Z} \bigoplus \mathbb{Z}_{p_1^{v_1}} \bigoplus \cdots \bigoplus \mathbb{Z}_{p_s^{vs}},$$

where $\mathbb{Z}$ is a cyclic group with infinite order and $\mathbb{Z}_{p_i^{v_i}}$ is a finite cyclic group of prime power order, for some prime p_i and some positive integer v_i.

Next we have the Number Theory portion of the preliminaries where we recall some basic definitions from this area. Throughout this thesis we will be dealing with several different of equations, some of which we describe as diophantine equations. Specifically, a *diophantine equation* is a type of equation that requires that the solutions come from the set of integers.

Additionally, we need to define the following notation and terms.

Definition 1.9. The *greatest common divisor* of two integers a and b, which are not both 0, is the largest integer that divides both a and b.

The notation that we use for the greatest common divisor of two integers a and b is $\gcd(a, b)$. For integers a and b we also use the notation $a|b$ to mean that a divides b and the notation $a \nmid b$ to mean that a does not divide b .

Definition 1.10. Let p be a prime number and n be a positive integer. If $p^a|n$ but $p^{a+1} \nmid n$, we say that p^a *exactly divides* n, and we write $p^a \parallel n$.

Another symbol that we should be aware of is $\div$, which we use to symbolize defined equality. Another symbol that we have already seen is $\equiv$, which defines a congruence. Along these lines we also need to define the term congruence class.

Definition 1.11. A *congruence class modulo m* contains integers that are mutually congruent modulo m.

For example the set of integers modulo 2 can be put into one of 2 congruence classes, namely the class of integers that are congruent to 0 modulo 2 or the class of integers that are congruent to 1 modulo 2 (a.k.a the class of even integers or the class of odd integers).

We conclude this section with the following two terms.

Definition 1.12. The *discriminant* of x^3+ax^2+bx+c is defined to be the quantity

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

Definition 1.13. Given a polynomial

$$P(x) = x^n + a_{n-1}x + \cdots + a_1x + a_0$$

of degree n with roots α_i, $i = 1, \ldots, n$ and a polynomial

$$Q(x) = x^m + b_{m-1}x + \cdots + b_1x + b_0$$

of degree m with roots β_j, $j = 1, \ldots, m$ the *resultant* $\rho(P, Q)$ is defined by

$$\rho(P, Q) = \prod_{i=1}^{n}\prod_{j=1}^{m}(\alpha_i - \beta_j).$$

Chapter 2

Congruent Numbers

2.1 Introduction

Before we dive into the topic of congruent numbers we recall, from Chapter 1, the most common definition of a congruent number.

Definition 2.1. A positive integer n is a *congruent number* if there exists a rational right angle triangle with area n.

We assume that the congruent numbers we are working with or searching for are square-free (except in Chapter 6 when we discuss the distribution of congruent numbers), since it is directly apparent from the definition of a congruent number that if n is a congruent number then so too is nk^2, for some integer k.

Additionally, there are several equivalent definitions for a congruent number, which can be summarized by the following theorem.

Theorem 2.2. *The following* 5 *statements are equivalent definitions for a positive integer* n *to be a congruent number.*

(i) There exist $x, y, z, t \in \mathbb{Z}^+$ *satisfying the rationalized Diophantine equations*

$$x^2 + ny^2 = z^2 \text{ and } x^2 - ny^2 = t^2,$$

as seen in [AC74, Alt80, Cha06, Kra86, God78, Tun83].

(ii) There exist $x, y, z \in \mathbb{Z}^+$ *satisfying the rationalized Diophantine equation*

$$x^4 - n^2y^4 = z^2, \qquad \text{as seen in [AC74].}$$

(iii) The elliptic curve

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

has non-trivial solutions $\in \mathbb{Q}$ *[Hem06, Cha06, Cip09, Ben02, Hem06, Kob92, Tun83].*

(iv) There exists a rational right angle triangle with area n [Cha06, NW93, Cip09, Coa05, Kra86, Nem98, DJS09, Ben02, Hem06, Ros05, Kob92, Tun83].

(v) There exist $u, v, w \in \mathbb{Z}^+$ with

$$nw^2 = uv(u^2 - v^2),$$

as seen in [AC74, Alt80, God78, Kra86, DJS09].

Proof. ($(i) \Rightarrow (ii)$) Assume that there exist $x, y, z, t, n \in \mathbb{Z}^+$ such that

$$x^2 + ny^2 = z^2 \tag{2.1}$$

and

$$x^2 - ny^2 = t^2. \tag{2.2}$$

Then multiplying Equations (2.1) and (2.2) gives us that

$$\begin{array}{rcl} (x^2 + ny^2)(x^2 - ny^2) & = & z^2t^2 \\ \Rightarrow \qquad x^4 - n^2y^4 & = & (zt)^2. \end{array}$$

Now, let $w = zt$ such that

$$x^4 - n^2y^4 = w^2$$

is solvable, which is exactly what we needed to show.

($(ii) \Rightarrow (iii)$) Assume that there exist $x, y, w, n \in \mathbb{Z}^+$ such that

$$x^4 - n^2y^4 = w^2.$$

Then

$$\begin{array}{rrcl} & x^4 - n^2y^4 & = & w^2 \\ \Rightarrow & \frac{x^4}{y^4} - n^2\frac{y^4}{y^4} & = & \dfrac{w^2}{y^4} \\ \Rightarrow & \left(\frac{x}{y}\right)^4 - n^2 & = & \left(\dfrac{w}{y^2}\right)^2 \\ \Rightarrow & \frac{x^2}{y^2}\left[\left(\frac{x}{y}\right)^4 - n^2\right] & = & \dfrac{x^2}{y^2}\left[\left(\dfrac{w}{y^2}\right)^2\right] \\ \Rightarrow & \left(\frac{x}{y}\right)^6 - n^2\frac{x^2}{y^2} & = & \left(\dfrac{wx}{y^3}\right)^2 \end{array}$$

Now, let $X = \frac{x^2}{y^2}$ and $Y = \frac{wx}{y^3}$ such that

$$\begin{array}{rrcl} & \left(\frac{x}{y}\right)^6 - n^2\frac{x^2}{y^2} & = & \left(\frac{wx}{y^3}\right)^2 \\ \Rightarrow & X^3 - n^2X & = & Y^2. \end{array}$$

This is exactly our elliptic curve definition, since X and Y are nonzero and thus nontrivial.

($(iii) \Rightarrow (iv)$) Assume that n is a positive integer and that there exist $X, Y \in \mathbb{Q}$ such that

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

Now, let $a = \frac{X^2-n^2}{Y}, b = \frac{2nX}{Y}$ and $c = \frac{X^2+n^2}{Y}$ so that

$$a^2 + b^2 = c^2.$$

Thus, we have a rational right angle triangle with sides a, b, c and area equal to n, since

$$\begin{array}{rcl} \frac{ab}{2} & = & \frac{(X^2-n^2)(2nX)}{2Y^2} \\ & = & \frac{n(X^3-n^2X)}{Y^2} \\ & = & \frac{nY^2}{Y^2} \\ & = & n. \end{array}$$

($(iv) \Rightarrow (v)$) Assume that n is a positive square-free integer and that there exists a right angle triangle with sides $a, b, c \in \mathbb{Q}$ such that

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

First, we can scale a, b, c to conclude that there exist $f, g, h \in \mathbb{Z}^+$ with

$$f^2 + g^2 = h^2, \qquad \text{where } f, g, h \text{ are relatively prime.}$$

Then, the area of this triangle would be

$$n = \frac{fg}{2}.$$

Now, using properties of pythagorean triples we know that there exist integers u and v such that $f = u^2 - v^2$, $g = 2uv$ and $h = u^2 + v^2$ [Dic20, Ros05]. Then

$$\begin{aligned} n &= \frac{2uv(u^2-v^2)}{2} \\ &= uv(u^2-v^2), \end{aligned}$$

which is exactly what we needed to show for the case when $w^2 = 1$. We note that a similar result occurs to include w^2 when n is not square-free[Cha98].

$((v) \Rightarrow (i))$ Assume that there exist $u, v, n, w \in \mathbb{Z}^+$ such that n is square-free,

$$nw^2 = uv(u^2 - v^2)$$

and $\gcd(u, v) = 1$ (or else we could divide out the gcd into w^2). Then clearly one of $u, v, u^2 - v^2$ is even and the other two are odd.

Case #1: Assume that u and v are odd then $u^2 - v^2$ is even. Next, let

$$\beta = 2uv \qquad \Rightarrow \;\; 2|\beta$$

and

$$\alpha = u^2 - v^2 \qquad \Rightarrow \;\; 2|\alpha, \text{ by assumption.}$$

Note that $\beta, \alpha \in \mathbb{Z}$, since $u, v \in \mathbb{Z}^+$. Then

$$nw^2 = \frac{\alpha\beta}{2}.$$

Now, let $y = w$ so that

$$ny^2 = \frac{\alpha\beta}{2}$$

and note that

$$x^2 = \left(\frac{u^2+v^2}{2}\right)^2 = \left(\frac{\alpha}{2}\right)^2 + \left(\frac{\beta}{2}\right)^2,$$

where x is in $\mathbb{Z}$ by definition of α and β. Then

$$\begin{aligned} ny^2 &= \frac{\alpha\beta}{2} \\ &= \frac{\alpha\beta}{2} + x^2 - x^2 \\ &= \frac{\alpha\beta}{2} + \left(\frac{\alpha}{2}\right)^2 + \left(\frac{\beta}{2}\right)^2 - x^2 \\ &= \left(\frac{\alpha}{2} + \frac{\beta}{2}\right)^2 - x^2. \end{aligned}$$

Therefore, let $z = \frac{\alpha}{2} + \frac{\beta}{2}$ (which is in $\mathbb{Z}$ by definition of α and β) such that

$$\begin{array}{rrcl} & ny^2 & = & \left(\frac{\alpha}{2} + \frac{\beta}{2}\right)^2 - x^2 \\ \Rightarrow & ny^2 & = & z^2 - x^2 \\ \Rightarrow & x^2 + ny^2 & = & z^2. \end{array}$$

Similarly,

$$\begin{aligned} x^2 &= \left(\frac{\alpha}{2}\right)^2 + \left(\frac{\beta}{2}\right)^2 \\ &= \left(\frac{\alpha}{2}\right)^2 + \left(\frac{\beta}{2}\right)^2 + ny^2 - ny^2 \\ &= \left(\frac{\alpha}{2}\right)^2 + \left(\frac{\beta}{2}\right)^2 + ny^2 - \frac{\alpha\beta}{2} \\ &= ny^2 + \left(\frac{\alpha}{2} - \frac{\beta}{2}\right)^2. \end{aligned}$$

So, let $t = \frac{\alpha}{2} - \frac{\beta}{2}$ (which is in $\mathbb{Z}$ by definition of α and β) such that

$$\begin{array}{rrcl} & x^2 & = & ny^2 + \left(\frac{\alpha}{2} - \frac{\beta}{2}\right)^2 \\ \Rightarrow & x^2 & = & ny^2 + t^2 \\ \Rightarrow & x^2 - ny^2 & = & t^2. \end{array}$$

Hence, we have obtained the rationalized Diophantine equations in (i) with $x, y, z, t \in \mathbb{Z}$, which can be restricted to $x, y, z, t \in \mathbb{Z}^+$.

Case #2: Assume that u is even and v is odd then $u^2 - v^2$ is odd. Next, we can make similar substitutions to obtain the same result.

Case #3: Similarly, when v is even and u is odd then $u^2 - v^2$ is odd and we obtain the same result.
This completes the proof.

□

Historically, the term "Congruent number" is a result of the equivalent definition stated in Theorem 2.2(i), since

$$x^2 + ny^2, x^2 - ny^2, \text{ and } x^2$$

are all congruent numbers modulo n [Cip09, Hem06, Kob92]. The most current definition of a congruent number is the one involving elliptic curves, as depicted in Theorem 2.2(iii) [Cip09]. This definition also gives us the term congruent number elliptic curve.

2.2 Families of Congruent Numbers

Since the 10th century several families of congruent numbers have been discovered. The purpose of this section is to present five families of congruent numbers, given in Alter and Curtz's paper [AC74], as well as proofs and examples for each.

Lemma 2.3. [AC74] *Given $a, b \in \mathbb{Z}^+$ if $n = a^4 + 4b^4$ then n is a congruent number.*

Proof. Given $n = a^4 + 4b^4$, for some $a, b \in \mathbb{Z}^+$, we need to show that there exist $x, y \in \mathbb{Z}^+$ such that

$$x^2 + ny^2 \qquad \text{and} \qquad x^2 - ny^2$$

are both squares. Now, for $n = a^4 + 4b^4$ we have

$$x^2 + ny^2 = x^2 + (a^4 + 4b^4)y^2 \tag{2.3}$$

and

$$x^2 - ny^2 = x^2 - (a^4 + 4b^4)y^2. \tag{2.4}$$

So, let $x = a^8 + 24a^4b^4 + 16b^8$ and $y = 4ab(4b^4 - a^4)$ in Equation (2.3) then

$$x^2 + (a^4 + 4b^4)y^2 = (a^8 + 24a^4b^4 + 16b^8)^2 + 16(a^4 + 4b^4)a^2b^2(4b^4 - a^4)^2 \tag{2.5}$$

and upon factoring (2.5) becomes

$$(a^8 + 32a^2b^6 - 8a^4b^4 + 8a^6b^2 + 16b^8)^2.$$

Similarly, when we let $x = a^8 + 24a^4b^4 + 16b^8$ and $y = 4ab(4b^4 - a^4)$ in Equation (2.4) we get that

$$x^2 - (a^4 + 4b^4)y^2 = (a^8 - 32a^2b^6 - 8a^4b^4 - 8a^6b^2 + 16b^8)^2.$$

Therefore, let

$$z = (a^8 + 32a^2b^6 - 8a^4b^4 + 8a^6b^2 + 16b^8)$$

and

$$t = (a^8 - 32a^2b^6 - 8a^4b^4 - 8a^6b^2 + 16b^8).$$

Then we have shown that there exist $x, y, z, t \in \mathbb{Z}^+$ such that $n = a^4 + 4b^4$ is a congruent number by Theorem 2.2(i).

□

Example 2.4. If we let $a = 1$ and $b = 2$ in Lemma 2.3 then $n = 1^4 + 4(2^4) = 65$ is a congruent number. Using Theorem 2.2 (i) we see that for $x = 97$ and $y = 12$

$$x^2 + 65(y^2) = 18769 = 137^2$$

and

$$x^2 - 65(y^2) = 49 = 7^2.$$

Hence, the rationalized Diophantine equations

$$x^2 + 65y^2 = z^2 \text{ and } x^2 - 65y^2 = t^2$$

are solvable with $x = 97, y = 12, z = 137$ and $t = 7$, which verifies that $n = 65$ is a congruent number.

Lemma 2.5. [AC74] *Given $a, b \in \mathbb{Z}^+$ if $n = 2a^4 + 2b^4$ then n is a congruent number.*

Proof. Given $n = 2a^4 + 2b^4$, for some $a, b \in \mathbb{Z}^+$, we need to show that there exist $x, y \in \mathbb{Z}^+$ such that

$$x^2 + ny^2 \qquad \text{and} \qquad x^2 - ny^2$$

are both squares. Now, for $n = 2a^4 + 2b^4$ we have

$$x^2 + ny^2 = x^2 + (2a^4 + 2b^4)y^2 \tag{2.6}$$

and

$$x^2 - ny^2 = x^2 - (2a^4 + 2b^4)y^2. \tag{2.7}$$

So, let $x = a^8 + 6a^4b^4 + b^8$ and $y = 2ab(a^4 - b^4)$ in Equation (2.6) then

$$x^2 + (2a^4 + 2b^4)y^2 = (a^8 + 6a^4b^4 + b^8)^2 + 4(2a^4 + 2b^4)a^2b^2(a^4 - b^4)^2 \tag{2.8}$$

and upon factoring (2.8) becomes

$$(a^8 + 4a^2b^6 - 2a^4b^4 + 4a^6b^2 + b^8)^2.$$

Similarly, when we let $x = a^8 + 6a^4b^4 + b^8$ and $y = 2ab(a^4 - b^4)$ in Equation (2.7) we get that

$$x^2 - (2a^4 + 2b^4)y^2 = (a^8 - 4a^2b^6 - 2a^4b^4 - 4a^6b^2 + b^8)^2.$$

Therefore, let

$$z = (a^8 + 4a^2b^6 - 2a^4b^4 + 4a^6b^2 + b^8)$$

and

$$t = (a^8 - 4a^2b^6 - 2a^4b^4 - 4a^6b^2 + b^8).$$

Then we have shown that there exist $x, y, z, t \in \mathbb{Z}^+$ such that $n = 2a^4 + 2b^4$ is a congruent number by Theorem 2.2(i).

□

Example 2.6. If we let $a = 1$ and $b = 2$ in Lemma 2.5 then $n = 2(1^4) + 2(2^4) = 34$ is a congruent number. Using Theorem 2.2(i) we see that for $x = 145$ and $y = 12$

$$x^2 + 34(y^2) = 25921 = 161^2$$

and

$$x^2 - 34(y^2) = 16129 = 127^2.$$

Hence, the rationalized Diophantine equations

$$x^2 + 34y^2 = z^2 \text{ and } x^2 - 34y^2 = t^2$$

are solvable with $x = 145, y = 12, z = 161$ and $t = 127$, which verifies that $n = 34$ is a congruent number.

Lemma 2.7. [AC74] *Given $a, b \in \mathbb{Z}^+$ if $n = a^4 - b^4$ then n is a congruent number.*

Proof. Given $n = a^4 - b^4$, for some $a, b \in \mathbb{Z}^+$, we need to show that there exist $x, y \in \mathbb{Z}^+$ such that

$$x^2 + ny^2 \qquad \text{and} \qquad x^2 - ny^2$$

are both squares. Now, for $n = a^4 - b^4$ we have

$$x^2 + ny^2 = x^2 + (a^4 - b^4)y^2 \tag{2.9}$$

and

$$x^2 - ny^2 = x^2 - (a^4 - b^4)y^2. \tag{2.10}$$

So, let $x = b^2(a^4 + b^4)$ and $y = 2ab^3$ in Equation (2.9) then

$$x^2 + (a^4 - b^4)y^2 = b^4(a^4 + b^4)^2 + 4(a^4 - b^4)a^2b^6 \tag{2.11}$$

and upon factoring (2.11) becomes

$$b^4(a^4 + 2a^2b^2 - b^4)^2.$$

Similarly, when we let $x = b^2(a^4 + b^4)$ and $y = 2ab^3$ in Equation (2.10) we get that

$$x^2 - (a^4 - b^4)y^2 = b^4(a^4 - 2a^2b^2 - b^4)^2.$$

Therefore, let $z = b^4(a^4 + 2a^2b^2 - b^4)^2$ and $t = b^4(a^4 - 2a^2b^2 - b^4)$ then we have shown that there exist $x, y, z, t \in \mathbb{Z}^+$ such that $n = a^4 - b^4$ is a congruent number by Theorem 2.2(i).

□

Example 2.8. If we let $a = 2$ and $b = 1$ in Lemma 2.7 then $n = 2^4 - 1^4 = 15$ is a congruent number. Using Theorem 2.2(i) we see that for $x = 17$ and $y = 4$

$$x^2 + 15y^2 = 529 = 23^2$$

and

$$x^2 - 15y^2 = 49 = 7^2.$$

Hence, the rationalized Diophantine equations

$$x^2 + 15y^2 = z^2 \text{ and } x^2 - 15y^2 = t^2$$

are solvable with $x = 17, y = 4, z = 23$ and $t = 7$, which verifies that $n = 15$ is a congruent number.

Lemma 2.9. [AC74] *For integers a and b with opposite parity if $nk^2 = a^4 + 6a^2b^2 + b^4$, for some integer k, then n is a congruent number.*

Proof. Recall by Theorem 2.2(v) that every congruent number n is of the form $nk^2 = uv(u^2 - v^2)$, with $k, u, v \in \mathbb{Z}^+$. So, let

$$u = f^2, \quad v = g^2, \quad u - v = h^2 \quad \text{and } u + v = nk^2$$

where $f, g, h, k, n \in \mathbb{Z}^+$. Then n is a congruent number since

$$uv(u^2 - v^2) = n(fghk)^2.$$

Now,

$$h^2 + g^2 = f^2 \qquad \text{(since u - v + v = u)}$$

is a pythagorean triple such that there exist $a, b \in \mathbb{Z}^+$ with

$$h = a^2 - b^2, \quad g = 2ab, \quad \text{and } f = a^2 + b^2, \tag{2.12}$$

where exactly one of a, b is even and the other is odd [Dic20, Ros05]. So, assume that h, g, f are defined as in (2.12) then

$$\begin{array}{rcl} f^2 + g^2 & = & nk^2 \\ \Rightarrow \qquad (a^2+b^2)^2 + (2ab)^2 & = & nk^2 \\ \Rightarrow \qquad a^4 + 6a^2b^2 + b^4 & = & nk^2. \end{array}$$

Hence, $nk^2 = a^4 + 6a^2b^2 + b^4$ is a family of congruent numbers when a and b have opposite parity.

□

Example 2.10. If we let $a = 1$ and $b = 2$ in Lemma 2.9 then $n = 1^4 + 6(1^2)(2^2) + 2^4 = 41$ is a congruent number. Using Theorem 2.2(i) we see that for $x = 881$ and $y = 120$

$$x^2 + 41y^2 = 1366561 = 1169^2$$

and

$$x^2 - 41y^2 = 185761 = 431^2.$$

Hence, the rationalized Diophantine equations

$$x^2 + 41y^2 = z^2 \text{ and } x^2 - 41y^2 = t^2$$

are solvable with $x = 881, y = 120, z = 1169$ and $t = 431$, which verifies that $n = 41$ is a congruent number.

Lemma 2.11. [AC74] *For integers a, b with opposite parity if $nk^2 = a^4 - 6a^2b^2 + b^4$ then n is a congruent number.*

Proof. Once again, recall by Theorem 2.2(v) that every congruent number n is of the form $nk^2 = uv(u^2 - v^2)$, with $k, u, v \in \mathbb{Z}^+$. So, let

$$u = f^2, \quad v = g^2, \quad u + v = h^2 \quad \text{and } u - v = nk^2$$

where $f, g, h, k, n \in \mathbb{Z}^+$. Then n is a congruent number since

$$uv(u^2 - v^2) = n(fghk)^2.$$

Now,

$$f^2 + g^2 = h^2$$

is a pythagorean triple such that there exist $a, b \in \mathbb{Z}^+$ with

$$f = a^2 - b^2, \quad g = 2ab, \quad \text{and } h = a^2 + b^2, \tag{2.13}$$

where exactly one of a, b is even and the other is odd [Dic20, Ros05]. So, assume that f, g, h are defined as in (2.13) then

$$\begin{array}{rccc} & f^2 - g^2 & = & nk^2 \\ \Rightarrow & (a^2 - b^2)^2 + (2ab)^2 & = & nk^2 \\ \Rightarrow & a^4 - 6a^2b^2 + b^4 & = & nk^2. \end{array}$$

Hence, $nk^2 = a^4 - 6a^2b^2 + b^4$ is a family of congruent numbers when a and b have opposite parity. □

Example 2.12. If we let $a = 4$ and $b = 1$ in Lemma 2.11 then $n = 4^4 - 6(4^2)(1^2) + 1^4 = 161$ is a congruent number. Using Theorem 2.2(i) we see that for $x = 305$ and $y = 24$

$$x^2 + 161y^2 = 185761 = 431^2$$

and

$$x^2 - 161y^2 = 289 = 17^2.$$

Hence, the rationalized Diophantine equations

$$x^2 + 161y^2 = z^2 \text{ and } x^2 - 161y^2 = t^2$$

are solvable with $x = 305, y = 24, z = 431$ and $t = 17$, verifying that $n = 161$ is a congruent number.

Chapter 3

Elliptic Curves

3.1 Introduction

Although elliptic curves do not resemble ellipses it is of some interest to note that the curves originated from the study of computing the arc length of an ellipse [ST93]. In general, an equation of the form

$$y^2 + axy + by = x^3 + cx^2 + dx + e,$$

with coefficients a, b, c, d and e in $\mathbb{Q}$, is an elliptic curve under certain restrictions. However, for our purposes we are primarily interested in a shorter form and as such define the following.

Definition 3.1 (Elliptic Curve in Weierstrass Normal Form)**.** An equation of the form

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

where a, b, and c are integers is an *elliptic curve* if the discriminant of $x^3 + ax^2 + bx + c$ is not 0 (i.e. the discriminant $D = -4a^3c + a^2b^2 + 18abc - 4b^3 - 27c^2 \neq 0$).

We note that the non-zero restriction on the discriminant of the cubic is necessary, since certain properties about elliptic curves do not hold otherwise. The discriminant requirement directly corresponds to a cubic with three distinct roots (real and/or complex). That is to say if the cubic, x^3+ax^2+bx+c, has a double root or a triple root then the equation $y^2 = x^3 + ax^2 + bx + c$ is not an elliptic curve. Examples of elliptic curves can be seen in Figure 3.1 and Figure 3.2 and examples of cubic equations with double and triple roots (and hence not elliptic curves) can be seen in Figure 3.3 and Figure 3.4, respectively.

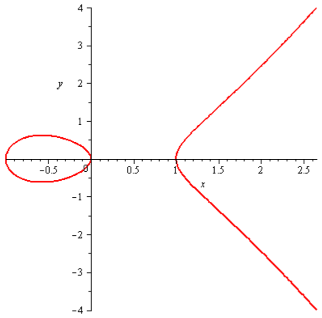

Figure 3.1: Elliptic curve with three real roots, $y^2 = x(x+1)(x-1)$.

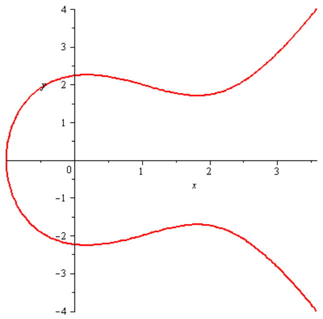

Figure 3.2: Elliptic curve with one real root, $y^2 = (x+1)(x^2-4x+5)$.

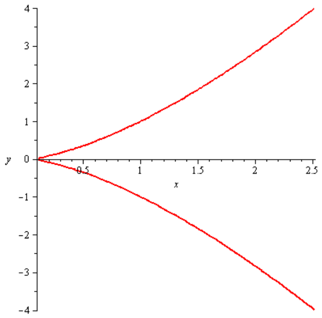

Figure 3.3: Cubic equation with a triple root, $y^2 = x^3$.

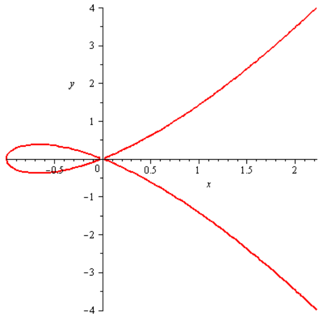

Figure 3.4: Cubic equation with a double root, $y^2 = x^2(x+1)$.

Given an elliptic curve E we are interested in the set of rational points on E, denoted by $E(\mathbb{Q})$. Before we can discuss the structure of $E(\mathbb{Q})$ we must define the group law associated with rational points on elliptic curves.

3.2 Group Law

Given two rational points on elliptic curve E can we find another rational point? The answer is yes. Before we can determine the other rational point, which is defined by the group law, we must first define the composition law.

So, let $E(\mathbb{Q})$ be the set of rational points on an elliptic curve E and let $*$ be the binary *composition law* operator that maps $E(\mathbb{Q}) \times E(\mathbb{Q})$ into $E(\mathbb{Q})$. Then for each $(P, Q) \in E(\mathbb{Q}) \times E(\mathbb{Q})$ we denote the element $*((P, Q))$ by

$P*Q$. We define $P*Q$ to be the third intersection point of the line PQ with the elliptic curve E [ST93, SZ03, Hus04, Sil86]. Similarly, if there is only one rational point P on the elliptic curve then we consider $P*P$ to be the third intersection point of the tangent line created at P with the elliptic curve E (where the tangent line is assumed to pass through the point P twice) [ST93, SZ03, Hus04, Sil86]. The composition law, also known as the chord and tangent method, is illustrated in Figure 3.5 and Figure 3.6 [Hus04].

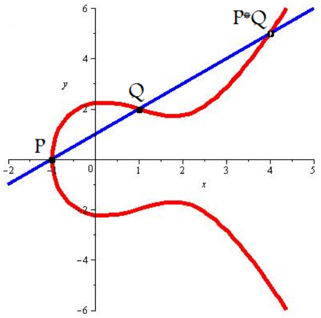

Figure 3.5: Geometric interpretation of $P*Q$ on the curve $y^2 = (x+1)(x^2-4x+5)$.

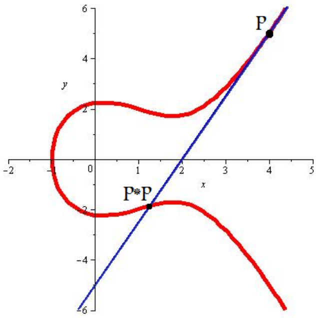

Figure 3.6: Geometric interpretation of $P*P$ on the curve $y^2 = (x+1)(x^2-4x+5)$.

Now, this might be all well and good but what if we do not even have one rational point on the elliptic curve? To solve this problem we assume that the elliptic curve has a rational point, known as the rational point at infinity, denoted by $\mathcal{O}$ [ST93, SZ03, Hus04, Sil86]. That is to say we assume that there exists at least one rational point on the elliptic curve E and call that point $\mathcal{O}$. Given this rational point at infinity we define $\mathcal{O}*\mathcal{O} = \mathcal{O}$ where the line at infinity meets the curve with multiplicity three at $\mathcal{O}$ [ST93, Sil86]. For some rational point P on E we also define $\mathcal{O}*P = P*\mathcal{O}$ to be the third point of intersection between the vertical line at P and the elliptic curve E [ST93, Sil86]. Specifically, $\mathcal{O}*P$ is the reflection of P about the x-axis [ST93].

We are now ready to introduce the binary *group law* operator + associated with $E(\mathbb{Q})$, where $\mathcal{O}$ is assumed to be the rational point at infinity on E. Assume that P and Q are rational points on E. Then we define $P+Q$ to be the reflection of $P*Q$ about the x-axis [ST93]. That is to say

$$P + Q = \mathcal{O} * (P * Q),$$

where $\mathcal{O}*(P*Q)$ is the third point of intersection on the vertical line through

$P * Q$ with the elliptic curve E. The group law operator is visually depicted in Figure 3.7.

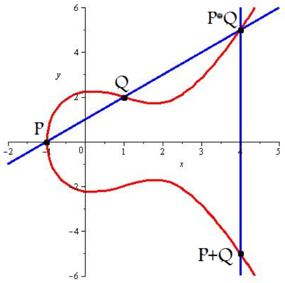

Figure 3.7: Geometric interpretation of $P + Q$ on the curve $y^2 = (x+1)(x^2 - 4x + 5)$.

Furthermore, given rational points P, Q and R on the elliptic curve E we also have the following rules associated with the group law operator, previously defined [ST93].

$$\begin{aligned} P + Q &= Q + P && \text{(commutative)} \\ P + \mathcal{O} = \mathcal{O} + P &= P && \text{(identity element } \mathcal{O}\text{)} \\ P + (-P) = (-P) + P &= \mathcal{O} && \text{(inverses)} \\ (P + Q) + R &= P + (Q + R) && \text{(associative),} \end{aligned}$$

where $-P$ is the notation for the reflection of P about the x-axis (i.e. $-P = \mathcal{O} * P$). These properties can be easily proved using the definition of the $+$ operator and the underlying $*$ operator (except the last one which requires a lengthy computation)[ST93]. It can also be shown that $E(\mathbb{Q})$ forms a group under $+$ [ST93]. Furthermore, Louis Mordell was able to elaborate on the structure of $E(\mathbb{Q})$ [ST93].

3.3 Mordell's Theorem

Given the preliminary background information in Abstract Algebra we recall the following theorem, which was proved in 1922 by Louis Mordell [tFE],

Theorem 3.2. [ST93, Hem06, Cha06, SZ03, Hus04, Sil86, Mordell's Theorem] *Let E be the elliptic curve given by*

$$E : y^2 = x^3 + ax^2 + bx,$$

where a and b are integers. Then the group of rational points $E(\mathbb{Q})$ is a finitely generated abelian group, under the group law operator $+$.

Proof. See [ST93, Chapter III], [Hus04, Chapter 6], or [Sil86, Chapter VIII]. □

In summary, Mordell's Theorem states that for an elliptic curve of the form $y^2 = x^3 + ax^2 + bx$, where a and b are integers, there exists a finite set of rational points that will generate all of the rational points on the elliptic curve using the group law operator, as defined in the previous section.

As a result of Mordell's Theorem, we can apply Theorem 1.8 to the group of rational points on an elliptic curve E, i.e.

$$E(\mathbb{Q}) \simeq \mathbb{Z} \bigoplus \cdots \bigoplus \mathbb{Z} \bigoplus \mathbb{Z}_{p_1^{v_1}} \bigoplus \cdots \bigoplus \mathbb{Z}_{p_s^{v_s}},$$

where $\mathbb{Z}$ is a cyclic group with infinite order and $\mathbb{Z}_{p_i^{v_i}}$ is a finite cyclic group of prime power order (for some prime p_i and some positive integer v_i) [ST93, Hem06, Cha06, SZ03, Hus04, Sil86]. This in turn leads us to the rank r of the elliptic curve E.

Definition 3.3. Let E be an elliptic curve with an associated finitely generated abelian group $E(\mathbb{Q})$. The number of generators with infinite order in $E(\mathbb{Q})$ is the *rank* r of the elliptic curve E.

For example let

$$E : y^2 = x^3 - 25x.$$

Then using the MAGMA code in Appendix B we find that

$$E(\mathbb{Q}) \simeq \mathbb{Z} \bigoplus \mathbb{Z}_2 \bigoplus \mathbb{Z}_2,$$

which implies that the rank of E is 1. Note that the group of rational points on an elliptic curve is finite if and only if the rank of the elliptic curve is 0 [ST93].

Now we already stated in Theorem 2.2 that an integer n is a congruent number if the elliptic curve $Y^2 = X^3 - n^2X$ has non-trivial rational solutions. This in turn directly relates to the following lemma.

Lemma 3.4. [Kob92, Hem06, DJS09, Ben02, Kra86, NW93, Nem98, Kob92] *A positive integer n is a congruent number if and only if the elliptic curve*

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

has rank at least 1.

Proof. See [Kob92, Chapter I Section 9], [Hem06, Chapter 2 Section 10], [Cha06], or [Kob92, Chapter I Section 9].

□

We provide the following example as reinforcement, since Lemma 3.4 will be a useful tool in later chapters.

Example 3.5. Consider,

$$E := y^2 = x^3 - 6^2x.$$

Using the MAGMA code in Appendix B we find that the rank of E is 1, thereby verifying that 6 is a congruent number by Lemma 3.4.

In the next chapter we present the method that we will be using to determine the rank of an elliptic curve.

Chapter 4

Rank Calculation

4.1 Method of 2-descent

Given an elliptic curve of the form $y^2 = x^3 + ax^2 + bx$ with $a, b \in \mathbb{Z}$ we can sometimes determine the rank of the curve using the 2-descent method described in this section [ST93].

We start by defining

$$E : y^2 = x^3 + ax^2 + bx \qquad \text{and} \qquad \overline{E} : y^2 = x^3 + \overline{a}x^2 + \overline{b}x$$

where $\overline{a} = -2a$ and $\overline{b} = a^2 - 4b$ [ST93]. The process of determining the rank of E requires that we look at both curves E and $\overline{E}$. So let Γ be the rational points on E and let $\overline{\Gamma}$ be the rational points on $\overline{E}$. Then for the multiplicative group of non-zero rational numbers, denoted by $\mathbb{Q}^*$, and the subgroup of squares of $\mathbb{Q}^*$, namely $\mathbb{Q}^{*2} = \left\{u^2 : u \in \mathbb{Q}^*\right\}$, define the homomorphisms [ST93]

$$\alpha : \Gamma \longrightarrow \frac{\mathbb{Q}^*}{\mathbb{Q}^{*2}} \qquad \text{and} \qquad \overline{\alpha} : \overline{\Gamma} \longrightarrow \frac{\mathbb{Q}^*}{\mathbb{Q}^{*2}}$$

such that

$$\alpha(P) = \begin{cases} 1 (\operatorname{mod} \mathbb{Q}^{*2}), & \text{for } P = \mathcal{O}, \\ b (\operatorname{mod} \mathbb{Q}^{*2}), & \text{for } P = (0,0), \\ x (\operatorname{mod} \mathbb{Q}^{*2}), & \text{for } P = (x,y) \end{cases}$$

and

$$\overline{\alpha}(P) = \begin{cases} 1 (\operatorname{mod} \mathbb{Q}^{*2}), & \text{for } P = \mathcal{O}, \\ \overline{b} (\operatorname{mod} \mathbb{Q}^{*2}), & \text{for } P = (0,0), \\ x (\operatorname{mod} \mathbb{Q}^{*2}), & \text{for } P = (x,y). \end{cases}$$

Then the rank r, of the elliptic curve E, satisfies the following equation [ST93]:

$$2^r = \frac{|\alpha(\Gamma)| \cdot |\overline{\alpha}(\overline{\Gamma})|}{4},$$

where $|\cdot|$ denotes the cardinality of set (i.e. the number of elements in the set). Using the definition of $\alpha(\Gamma)$ and $\overline{\alpha}(\overline{\Gamma})$, to find elements in each set we need to find rational numbers on the respective elliptic curves where the x coordinates are distinct modulo squares.

As another perspective, Silverman and Tate state that the group $\alpha(\Gamma)$ consists, modulo $\mathbb{Q}^{*2}$, of at least 1 and b. They also state that $\alpha(\Gamma)$ contains all divisors b_1 of b, as long as $b_1 \not\equiv 1, b (\operatorname{mod} \mathbb{Q}^{*2})$ and the equation

$$N^2 = b_1 M^4 + aM^2e^2 + b_2e^4 \qquad \text{where } b = b_1b_2$$

has an integral solution $(N, M, e) \in \mathbb{Z}$, with the restriction that $M \neq 0, e \neq 0$ and $\gcd(M, e) = \gcd(N, e) = \gcd(b_1, e) = \gcd(b_2, M) = \gcd(M, N) = 1$ [ST93].

Similarly, the group $\overline{\alpha}(\overline{\Gamma})$ consists, modulo $\mathbb{Q}^{*2}$, of $1, \overline{b}$, and all divisors $\overline{b_1}$ of $\overline{b}$, as long as $\overline{b_1} \not\equiv 1, \overline{b} (\operatorname{mod} \mathbb{Q}^{*2})$ and the equation

$$\begin{aligned} N^2 &= \overline{b_1}M^4 + \overline{a}M^2e^2 + \overline{b_2}e^4 && \text{where } \overline{b} = \overline{b_1}\ \overline{b_2} \\ &= \overline{b_1}M^4 - 2aM^2e^2 + \overline{b_2}e^4 && \text{since } a = -2a \end{aligned}$$

has an integral solution $(N, M, e) \in \mathbb{Z}$ [ST93]. We also require that $M \neq 0, e \neq 0$ and $\gcd(M, e) = \gcd(N, e) = \gcd(\overline{b_1}, e) = \gcd(\overline{b_2}, M) = \gcd(M, N) = 1$ [ST93].

Altogether, this gives us a method for determining the rank of E, provided that we are able to determine if each of the curves generated by the divisors of b and $\overline{b}$ have solutions or not. It is also important to note that calculating the rank of an elliptic curve using the 2-descent method can be rather time consuming, depending on how many square free divisors there are of b and $\overline{b}$.

In addition, we can apply the following theorem to easily determine all of the rational points of finite order on E.

Theorem 4.1. [ST93, Cha06, Sil86, Nagell-Lutz Theorem] *Let*

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

be an elliptic curve with integer coefficients; and let D be the discriminant of the cubic polynomial $f(x)$

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

Let $P = (x, y)$ be a rational point of finite order, also known as a torsion point. Then x and y are integers and either $y = 0$, in which case P has order two, or else y divides D.

Proof. See [ST93, Chapter II], or [Sil86, Chapter VIII]. □

We note that the Nagell-Lutz' Theorem is not an if and only if statement [ST93]. That is to say for each of the rational points $P = (x, y)$ that satisfy $y = 0$ or y divides D we need to check that there exists an integer $n \geq 1$ such that $nP = 0$, in order to verify that P has finite order [ST93]. All in all, using the 2-descent (if successful) and the possible points of finite order from Nagell-Lutz' Theorem we can fully determine the group structure for $E(\mathbb{Q})$.

4.2 Worked Example

To re-enforce the 2-descent method we provide the following example.

Example 4.2. Determine the rank of $y^2 = x^3 - 23^2x$.

Solution: Using the 2-descent method we need to find all elements of $\alpha(\Gamma)$ and $\overline{\alpha}(\overline{\Gamma})$ when $a = 0, b = -23^2, \overline{a} = 0$ and $\overline{b} = 4 \cdot (23^2)$.

Given $b = b_1b_2$, we know that $\alpha(\Gamma)$ contains $b (\operatorname{mod} \mathbb{Q}^{*2})$, and $b_1 (\operatorname{mod} \mathbb{Q}^{*2})$ when there exist $N, M, e \in \mathbb{Z}$ such that

$$N^2 = b_1M^4 + aM^2e^2 + b_2e^4$$

with $M \neq 0$. In our case $b = -23^2$ such that the divisors of b are $\pm 1, \pm 23$ and $\pm 23^2$. However, $23^2 \equiv 1 (\operatorname{mod} \mathbb{Q}^{*2})$ and $-23^2 \equiv -1 (\operatorname{mod} \mathbb{Q}^{*2})$ so we need only consider $b_1 = 1, -1, 23, -23$. Since, $b (\operatorname{mod} \mathbb{Q}^{*2})$ and 1 are automatically in $\alpha(\Gamma)$ we get that $-1, 1 \in \alpha(\Gamma)$.

For the remaining b_1 values consider the following equations:

(i) $N^2 = -23M^4 + 23e^4$

(ii) $N^2 = 23M^4 - 23e^4$.

Clearly, the solution $(N, M, e) = (0, 1, 1)$ satisfies both of the above equations such that

$$\begin{array}{rrcll} & \alpha(\Gamma) & = & \{1, -1, 23, -23\} & (4.1) \\ \Rightarrow & |\alpha(\Gamma)| & = & 4 & (4.2) \end{array}$$

Similarly, for $\overline{b} = \overline{b_1}\ \overline{b_2}$ we know that $\overline{\alpha}(\overline{\Gamma})$ contains $\overline{b} (\operatorname{mod} \mathbb{Q}^{*2})$, and $\overline{b_1} (\operatorname{mod} \mathbb{Q}^{*2})$ when the equation

$$N^2 = \overline{b_1}M^4 + \overline{a}M^2e^2 + \overline{b_2}e^4$$

has an integral solution with $M \neq 0$. Now, upon removing squares we get that the square free divisors of $\overline{b}$ are $\pm 1, \pm 2, \pm 23$ and ± 46. Since, $\overline{b} (\bmod \mathbb{Q}^{*2})$ is automatically in $\overline{\alpha}(\overline{\Gamma})$ we get that $1 \in \overline{\alpha}(\overline{\Gamma})$. We now consider the following equations:

(i) $N^2 = -M^4 - 4 \cdot 23^2 e^4$

(ii) $N^2 = 2M^4 + 2 \cdot 23^2 e^4$

(iii) $N^2 = -2M^4 - 2 \cdot 23^2 e^4$

(iv) $N^2 = 23M^4 + 4 \cdot 23e^4$

(v) $N^2 = -23M^4 - 4 \cdot 23e^4$

(vi) $N^2 = 2 \cdot 23M^4 + 2 \cdot 23e^4$

(vii) $N^2 = -2 \cdot 23M^4 - 2 \cdot 23e^4$.

Clearly, $N^2 \geq 0$ and we require $M \neq 0$ such that Equations $(i), (iii), (v), (vii)$ will not have any integer solutions and can therefore be eliminated. Using the MAPLE$^{\text{TM}}$ code in Appendix A we find that $(N, M, e) = (410, 17, 1)$ is a valid solution for Equation (ii) such that $2 \in \overline{\alpha}(\overline{\Gamma})$.

So far we have that

$$\overline{\alpha}(\overline{\Gamma}) = \{1, 2\}.$$

However, the remaining equations, (iv) and (vi), are a little bit harder to solve, namely because they actually do not contain solutions. Our approach will be to show that one of the remaining equations does not have a solution. Then we can apply the fact that the $|\overline{\alpha}(\overline{\Gamma})|$ must be a power of 2 such that the other equation cannot have solutions either.

From Equation (iv) we see that

$$\begin{array}{rrcl} & N^2 & \equiv & 3M^4 (\bmod 4) \\ \Rightarrow & N^2 & \equiv & 3 (\bmod 4), \end{array}$$

since the $\gcd(\overline{b_2}, M) = 1$ we must have that M is odd and not divisible by 4 such that $M^4 \equiv 1 (\bmod 4)$. However, $N^2 \equiv 3 (\bmod 4)$ has no solutions, so we can conclude that $N^2 = 23M^4 + 4 \cdot 23e^4$ has no solutions. This in turn allows us to conclude that Equation (vi) must also have no solutions. Therefore,

$$\begin{array}{rrcl} & \overline{\alpha}(\overline{\Gamma}) & = & \{1, 2\} \qquad (4.3) \\ \Rightarrow & |\overline{\alpha}(\overline{\Gamma})| & = & 2 \qquad (4.4) \end{array}$$

so that

$$2^r = \frac{|\alpha(\Gamma)| \cdot |\overline{\alpha}(\overline{\Gamma})|}{4} = \frac{4 \cdot 2}{4} = 2^1.$$

Thus, the rank of $y^2 = x^3 - 23^2x$ is 1. Note that we could have also determined rational points on E or $\overline{E}$ such that the x coordinate, modulo squares, would be in Γ or $\overline{\Gamma}$, respectively.

Chapter 5

Congruent Number Curves of Moderate Rank

The purpose of this chapter is to present an infinite family of congruent number elliptic curves having moderate rank. In our case, the term moderate rank means rank at least three. In Section 5.1 we present the main theorem for this chapter, as well as some preliminary results, followed by Section 5.2 which contains the proof to the main theorem.

Now, it may not seem very beneficial to find an infinite family of congruent number elliptic curve with rank at least three but it turns out that even general elliptic curves with rank at least three are rare. Using a typical sample set of all elliptic curves A. Brumer and O. McGuinness studied the ranks of 310716 elliptic curves to find that only 4.08% of these curves have rank at least 3 [BM90]. We also note that the largest known rank for a congruent number elliptic curve is 6 [DJS09], which re-enforces the significance of finding infinitely many congruent number elliptic curves with rank at least 3.

5.1 Rank Three Results

To start, we present the main result for this chapter in the following theorem.

Theorem 5.1. [JS] *The curve*

$$w^2 = t^4 + 14t^2 + 4$$

has infinitely many rational points. Let (t, w) with $t \neq 0$ be one of them. Set $t = u/v$ where u and v are integers with $\gcd(u, v) = 1$. Define the positive integer n by

$$n = 6(u^4 + 2u^2v^2 + 4v^4)(u^4 + 8u^2v^2 + 4v^4). \tag{5.1}$$

Then the congruent number elliptic curve $y^2 = x(x^2 - n^2)$ has rank at least three.

We provide the following example, not as proof of Theorem 5.1 but to illustrate the results.

Example 5.2. The point $(t, w) = \left(\frac{1}{2}, \frac{11}{4}\right)$ is on the curve

$$w^2 = t^4 + 14t^2 + 4.$$

Then by Theorem 5.1 let $u = 1$ and $v = 2$ such that $n = 42486$. Using the MAGMA code in Appendix B we find that the curve

$$y^2 = x^3 - 42486^2 x$$

has rank of at least 3. Note that the actual output from MAGMA is "Warning: rank computed (3) is only a lower bound (It may still be correct, though)". However, since Theorem 5.1 is only stating a rank of at least three these results do coincide with the theorem.

Before we prove Theorem 5.1 in Section 5.2 we will need the following helpful lemmas.

Lemma 5.3. [JS] *If u and v are integers with* $\gcd(u, v) = 1$ *then the quantities*

(i) $\pm 6(u^4 + 2u^2v^2 + 4v^4)(u^4 + 8u^2v^2 + 4v^4)$

(ii) $\pm 6(u^4 + 2u^2v^2 + 4v^4)$

(iii) $\pm 2(u^4 + 2u^2v^2 + 4v^4)(u^4 + 8u^2v^2 + 4v^4)$

(iv) $\pm 2(u^4 + 2u^2v^2 + 4v^4)$

are not equal to squares in $\mathbb{Q}$.

Proof. The proof for each case is similar so we will prove Case i) in detail and summarize the other three cases accordingly.

Case i) Assume that u and v are integers such that the $\gcd(u, v) = 1$. Then we need to show that

$$\pm 6(u^4 + 2u^2v^2 + 4v^4)(u^4 + 8u^2v^2 + 4v^4) \tag{5.2}$$

is not a square in $\mathbb{Q}$. The only subcase that we need to consider is the subcase where u is even and v is odd, since we require that $\gcd(u, v) = 1$ and we see that the other three subcases either cannot occur or by properties of even and odd addition and multiplication will result in

$$2 \parallel \pm 6(u^4 + 2u^2v^2 + 4v^4)(u^4 + 8u^2v^2 + 4v^4),$$

which clearly implies that $\pm 6(u^4 + 2u^2v^2 + 4v^4)(u^4 + 8u^2v^2 + 4v^4)$ is not a square in $\mathbb{Q}$.

So, assuming that u is even and v is odd we can let $u = 2k$ for some $k \in \mathbb{Z}$ and apply properties of even and odd numbers such that (5.2) becomes

$$\pm 6(2^4k^4 + 2^3k^2v^2 + 4v^4)(2^4k^4 + 2^5k^2v^2 + 4v^4).$$

Hence,

$$2^5 \parallel \pm 6(u^4 + 2u^2v^2 + 4v^4)(u^4 + 8u^2v^2 + 4v^4),$$

since we can factor out 2^5 and the remaining factors

$$3, (2^2k^4 + 2k^2v^2 + v^4) \text{ and } (2^2k^4 + 2^3k^2v^2 + v^4)$$

are odd, so that

$$\pm 3(2^2k^4 + 2k^2v^2 + v^4)(2^2k^4 + 2^3k^2v^2 + v^4)$$

must also be odd. Therefore, $\pm 6(u^4 + 2u^2v^2 + 4v^4)(u^4 + 8u^2v^2 + 4v^4)$ is not a square in $\mathbb{Q}$.

Case ii) Similarly, for integers u and v assume that the $\gcd(u, v) = 1$ with u even and v odd. Then

$$2^3 \parallel \pm 6(u^4 + 2u^2v^2 + 4v^4),$$

so that $\pm 6(u^4 + 2u^2v^2 + 4v^4)$ is not a square in $\mathbb{Q}$.

Case iii) Once again, assume that u and v are integers such that $\gcd(u, v) = 1$ with u even and v odd. Then

$$2^5 \parallel \pm 2(u^4 + 2u^2v^2 + 4v^4)(u^4 + 8u^2v^2 + 4v^4),$$

so that $\pm 2(u^4 + 2u^2v^2 + 4v^4)(u^4 + 8u^2v^2 + 4v^4)$ is not a square in $\mathbb{Q}$.

Case iv) Lastly, assume that u and v are integers such that the $\gcd(u, v) = 1$ with u even and v odd. Then

$$2^3 \parallel \pm 2(u^4 + 2u^2v^2 + 4v^4),$$

so that $\pm 2(u^4 + 2u^2v^2 + 4v^4)$ is not a square in $\mathbb{Q}$.

□

Lemma 5.4. [JS] *If u and v are nonzero integers with* $\gcd(u,v)=1$ *then the quantities*

(i) $\pm(u^4+2u^2v^2+4v^4)$

(ii) $\pm(u^4+8u^2v^2+4v^4)$

are not equal to squares in $\mathbb{Q}$.

Proof. Clearly, if u and v are nonzero integers with $\gcd(u,v)=1$ then the only possible way for any of the quantities

(i) $\pm(u^4+2u^2v^2+4v^4)$

(ii) $\pm(u^4+8u^2v^2+4v^4)$

to be squares would occur in the positive cases of (i) and (ii). So, by way of contradiction assume that one of the quantities is a square such that

$$(u^4+2u^2v^2+4v^4) \quad = \quad z_1^2$$

or

$$(u^4+8u^2v^2+4v^4) \quad = \quad z_2^2,$$

for some $z_1, z_2 \in \mathbb{Z}$. Equivalently, either

$$\begin{aligned} \frac{u^2}{v^6}(u^4+2u^2v^2+4v^4) &= z_1^2\frac{u^2}{v^6} \\ \Rightarrow \qquad \frac{u^6}{v^6}+\frac{2u^4}{v^4}+\frac{4u^2}{v^2} &= \frac{z_1^2u^2}{v^6} \end{aligned}$$

or

$$\begin{aligned} \frac{u^2}{v^6}(u^4+8u^2v^2+4v^4) &= z_2^2\frac{u^2}{v^6} \\ \Rightarrow \qquad \frac{u^6}{v^6}+\frac{8u^4}{v^4}+\frac{4u^2}{v^2} &= \frac{z_2^2u^2}{v^6}. \end{aligned}$$

Now, let $x=\frac{u^2}{v^2}$ and $y_i=\frac{z_iu}{v^3}$, for $i=1,2$, be the rational points on the above curves. Then by substitution either

$$x^3+2x^2+4x \quad = \quad y_1^2 \tag{5.3}$$

or

$$x^3 + 8x^2 + 4x \quad = \quad y_2^2, \tag{5.4}$$

respectively, such that (5.3) and (5.4) are elliptic curves by definition. Using the MAGMA code in Appendix B we find that the rank of both (5.3) and (5.4) is 0. This in turn gives us that there is a finite number of rational points on (5.3) and (5.4), by Theorem 3.2.

Once again using the MAGMA code in Appendix B we find that the only finite rational point on (5.3) is $(x, y) = (0, 0)$. This, however, is not a valid solution for $x = \frac{u^2}{v^2}$ since u is required to be a nonzero integer. Similarly, we also have that the only finite rational points on (5.4) are $(0, 0), (-2, 4)$ and $(-2, -4)$, of which none correspond to a nonzero $x = u^2/v^2$ with u and v being integers. Hence, there does not exist $z_1, z_2 \in \mathbb{Z}$ such

$$(u^4 + 2u^2v^2 + 4v^4)$$

or

$$(u^4 + 8u^2v^2 + 4v^4)$$

are squares in $\mathbb{Q}$.

□

Lemma 5.5. [JS] *For integers u, v such that the* $\gcd(u, v) = 1$ *we have*

(i) $3 \nmid (u^4 + 8u^2v^2 + 4v^4)$,

(ii) $3 \nmid (u^4 + 2u^2v^2 + 4v^4)$.

Proof. Let u, v be integers such that the $\gcd(u, v) = 1$. Then we need to show that 3 does not divide either of the quantities $(u^4 + 8u^2v^2 + 4v^4)$ or $(u^4 + 2u^2v^2 + 4v^4)$. First, consider each of the quantities modulo 3 such that

$$\begin{aligned}(u^4 + 8u^2v^2 + 4v^4) &\equiv (u^4 + 2u^2v^2 + v^4) \pmod 3 \\ &\equiv (u^2 + v^2)^2 \pmod 3\end{aligned}$$

and

$$\begin{aligned}(u^4 + 2u^2v^2 + 4v^4) &\equiv (u^4 + 2u^2v^2 + v^4) \pmod 3 \\ &\equiv (u^2 + v^2)^2 \pmod 3.\end{aligned}$$

Note that both of the quantities are congruent to $(u^2 + v^2)^2$ modulo 3. It remains to show that 3 does not divide $(u^2 + v^2)^2$.

By way of contradiction assume that 3 does divide $(u^2+v^2)^2$. Then

$$(u^2+v^2)^2 \equiv 0 (\operatorname{mod} 3). \tag{5.5}$$

Considering squares modulo 3, for some $x \in \{0,1,2\}$, we have that $x^2 \equiv 0 (\operatorname{mod} 3)$ when $x=0$ and $x \equiv 1 (\operatorname{mod} 3)$ when $x = 1, 2$. Therefore,

$$\begin{array}{rccc} & (u^2+v^2)^2 & \equiv & 0 (\operatorname{mod} 3) \\ \Rightarrow & u^2+v^2 & \equiv & 0 (\operatorname{mod} 3) \\ \Rightarrow & u^2 \equiv v^2 & \equiv & 0 (\operatorname{mod} 3). \end{array}$$

This however yields a contradictions since $\gcd(u,v) = 1$, by assumption. Therefore 3 does not divide $(u^2+v^2)^2$ which is enough to show that 3 does not divide $(u^4+8u^2v^2+4v^4)$ or $(u^4+2u^2v^2+4v^4)$.

□

Lemma 5.6. [JS] *For integers u, v with* $\gcd(u,v) = 1$, *neither of the following quantities is equal to a square in* $\mathbb{Q}$.

$$\pm(u^4+2u^2v^2+4v^4)(u^4+8u^2v^2+4v^4).$$

Proof. Clearly, $-(u^4+2u^2v^2+4v^4)(u^4+8u^2v^2+4v^4)$ cannot be a square in $\mathbb{Q}$. It remains to show that

$$(u^4+2u^2v^2+4v^4)(u^4+8u^2v^2+4v^4) \tag{5.6}$$

is not a square in $\mathbb{Q}$.

We start by showing that if (5.6) is a square in $\mathbb{Q}$ then this would require that each of

$$(u^4+2u^2v^2+4v^4) \tag{5.7}$$

and

$$(u^4+8u^2v^2+4v^4) \tag{5.8}$$

must be squares in $\mathbb{Q}$. In order to show that each of the factors is a square we consider the resultant of (5.7) and (5.8), since we can use the resultant of two factors to find all possible greatest common divisors (gcds) of the two factors (as seen in [Wal05]). We can then use the possible gcds to show that each of the factors only have squares in common.

Using the MAPLE$^{\text{TM}}$ code in Appendix A we find that the resultant of these factors is $20736v^{16}$, with respect to u, and $20736u^{16}$, with respect to

v. This in turn implies that either 2 and/or 3 must divide (5.7) and (5.8), since $20736 = 2^8 3^4$ and $\gcd(u, v) = 1$.

Recall from Lemma 5.5 that 3 does not divide (5.7) or (5.8). Also, if 2 does divide (5.7) and (5.8) then this would imply that u is even and v is odd, which directly gives us that 4 exactly divides (5.7) and 4 exactly divides (5.8). However, 4 is a square which is enough to show that if (5.6) is a square in $\mathbb{Q}$ then each of (5.7) and (5.8) must be squares in $\mathbb{Q}$.

Finally, using Lemma 5.4 we see that each of $(u^4 + 2u^2v^2 + 4v^4)$ and $(u^4 + 8u^2v^2 + 4v^4)$ cannot be squares in $\mathbb{Q}$ so that $(u^4 + 2u^2v^2 + 4v^4)(u^4 + 8u^2v^2 + 4v^4)$ is not a square in $\mathbb{Q}$.

□

Lemma 5.7. [JS] *There exist infinitely many pairs of rational numbers (t, w) such that*

$$w^2 = t^4 + 14t^2 + 4.$$

Proof. We need to show that there exist infinitely many rational points on the curve

$$w^2 = t^4 + 14t^2 + 4. \tag{5.9}$$

Equivalently, we can show that there exist infinitely many rational points on the elliptic curve

$$Y^2 = X^3 - 6588X + 39312,$$

since the MAPLE$^{\text{TM}}$ code in Appendix A shows that the two curves are birationally equivalent. Recall that an elliptic curve contains infinitely many rational points if the rank of the elliptic curve is at least 1. Using the MAGMA code in Appendix B we find that rank of $Y^2 = X^3 - 6588X + 39312$ is 1. Hence, $w^2 = t^4 + 14t^2 + 4$ contains infinitely many rational points.

□

5.2 Proof of the Main Theorem

We are now prepared to prove Theorem 5.1.

Proof. Recall from Lemma 5.7 that the curve

$$w^2 = t^4 + 14t^2 + 4 \tag{5.10}$$

has infinitely many rational points. Now, let (t, w) be a rational point on (5.10) with $t \neq 0$, and set $t = u/v$ where u and v are integers with $\gcd(u, v) = 1$. Then for

$$n = 6(u^4 + 2u^2v^2 + 4v^4)(u^4 + 8u^2v^2 + 4v^4)$$

it remains to show that the curve

$$y^2 = x^3 - n^2x \tag{5.11}$$

has rank, r, at least three. Using the 2-descent method described in Chapter 4 it is enough to show that $2^r \geq 8$, since this would imply that r is at least 3. More specifically, since

$$2^r = \frac{|\alpha(\Gamma)| \cdot |\overline{\alpha}(\overline{\Gamma})|}{4}$$

we will show that $|\alpha(\Gamma)| \geq 32$.

As described in Chapter 4 let Γ be the group of rational points on the elliptic curve $y^2 = x^3 - n^2x$ and let $\overline{\Gamma}$ be the group of rational point on the elliptic curve $y^2 = x^3 + 4n^2x$. Then we need to find as many elements of $\alpha(\Gamma)$ and $\overline{\alpha}(\overline{\Gamma})$ where

$$\alpha(P) = \begin{cases} 1 (\operatorname{mod} \mathbb{Q}^{*2}), & \text{for } P = \mathcal{O}, \\ b (\operatorname{mod} \mathbb{Q}^{*2}), & \text{for } P = (0,0), \\ x (\operatorname{mod} \mathbb{Q}^{*2}), & \text{for } P = (x,y) \end{cases}$$

and

$$\overline{\alpha}(P) = \begin{cases} 1 (\operatorname{mod} \mathbb{Q}^{*2}), & \text{for } P = \mathcal{O}, \\ \overline{b} (\operatorname{mod} \mathbb{Q}^{*2}), & \text{for } P = (0,0), \\ x (\operatorname{mod} \mathbb{Q}^{*2}), & \text{for } P = (x,y), \end{cases}$$

as defined in Chapter 4.

By definition, $\alpha(\Gamma)$ contains $b (\operatorname{mod} \mathbb{Q}^{*2})$. Also recall that, for $b = b_1b_2$, $\alpha(\Gamma)$ contains $b_1 (\operatorname{mod} \mathbb{Q}^{*2})$ when the equation

$$N^2 = b_1M^4 + aM^2e^2 + b_2e^4$$

has a solution with $M \neq 0$. In our case $b = -n^2$ such that the divisors of b include $\pm 1, \pm n$ and $\pm n^2$, plus the divisors of n. However, $n^2 \equiv 1 (\operatorname{mod} \mathbb{Q}^{*2})$ and $-n^2 \equiv -1 (\operatorname{mod} \mathbb{Q}^{*2})$ such that $-1, 1 \in \alpha(\Gamma)$, and we need to only consider $b_1 = n, -n$ and all other divisors of n.

So, for $b_1 = n$ and $b_1 = -n$ consider the following equations:

(i) $N^2 = nM^4 - ne^4$

(ii) $N^2 = -nM^4 + ne^4$.

Clearly, the solution $(N, M, e) = (0, 1, 1)$ satisfies both of the above equations. Furthermore, Lemma 5.3(i) shows that n is not a square such that $n, -n \in \alpha(\Gamma)$. So far we have

$$\alpha(\Gamma) \;\supseteq\; \{1, -1, n, -n\}\,.$$

To find more elements of $\alpha(\Gamma)$ we consider the following non-torsion points, that satisfy $y^2 = x^3 - n^2x$,

$$\begin{aligned}
P_1 &= (x,y) = \left(-36u^2v^2(u^4+8u^2v^2+4v^4), 36uv(u^2-2v^2)(u^4+8u^2v^2+4v^4)^2\right),\\
P_2 &= (x,y) = \left(12(u^4+2u^2v^2+4v^4)^2, 36(u^4-4v^4)(u^4+2u^2v^2+4v^4)^2\right),\\
P_3 &= (x,y) = \left(-36u^2v^2(u^4+2u^2v^2+4v^4), 36uv^3\left(u^4+2u^2v^2+4v^4\right)^2 w\right).
\end{aligned}$$

It is easy to show that P_1 and P_2 are on $y^2 = x^3 - n^2x$, just make direct substitutions for x and y. For P_3 we need to recall that $w^2 = t^4 + 14t^2 + 4$ and $t = u/v$ such that

$$\begin{aligned}
& y^2 &=& \; (-36u^2v^2(u^4+8u^2v^2+4v^4))^3 - n^2(-36u^2v^2(u^4+8u^2v^2+4v^4))\\
\Rightarrow\; & y^2 &=& \; 1296u^2v^2(u^4+14u^2v^2+4v^4)(u^4+2u^2v^2+4v^4)^4\\
\Rightarrow\; & \tfrac{y^2}{v^4} &=& \; 36^2u^2v^2\left(\left(\frac{u}{v}\right)^4+14\left(\frac{u}{v}\right)^2+4\right)(u^4+2u^2v^2+4v^4)^4\\
\Rightarrow\; & \tfrac{y^2}{v^4} &=& \; 36^2u^2v^2(t^4+14t^2+4)(u^4+2u^2v^2+4v^4)^4\\
\Rightarrow\; & y^2 &=& \; 36^2u^2v^6w^2(u^4+2u^2v^2+4v^4)^4\\
\Rightarrow\; & y &=& \; \pm 36uv^3w(u^4+2u^2v^2+4v^4)^2.
\end{aligned}$$

It remains to show that P_1, P_2 and P_3 are not congruent modulo $\mathbb{Q}^{*2}$ to each other or any of the other points already in $\alpha(\Gamma)$. To start, consider

$$\alpha(P_1) \equiv -(u^4+8u^2v^2+4v^4)(\operatorname{mod}\mathbb{Q}^{*2}).$$

Then using Lemma 5.4 (ii) we see that $\pm(u^4+8u^2v^2+4v^4)$ is not a square in $\mathbb{Q}$ such that $-(u^4+8u^2v^2+4v^4) \subseteq \alpha(\Gamma)$, since clearly $\pm(u^4+8u^2v^2+4v^4)$ is not congruent to ± 1 or $\pm n$. Using Lemma 5.3(ii) we see that $\pm\alpha(P_1)n$ is not a square in $\mathbb{Q}$ either such that

$$\alpha(\Gamma) \supseteq S_1 \doteqdot \left\{\pm 1, \pm n, \pm(u^4+8u^2v^2+4v^4), \pm n(u^4+8u^2v^2+4v^4)\right\}.$$

Now, consider

$$\alpha(P_2) \equiv 3(\operatorname{mod} \mathbb{Q}^{*2}).$$

Then clearly 3 is not a square in $\mathbb{Q}$, however it remains to show that $\alpha(P_2) \not\equiv s(\operatorname{mod} \mathbb{Q}^{*2})$ for all $s \in S_1$. So, consider the case where the congruence holds then there would exist integers c_1, c_2 with $c_1, c_2 \in \{0, 1\}$ such that

$$\begin{array}{rcl} \alpha(P_2) & \equiv & \pm n^{c_1} \left(u^4 + 8u^2v^2 + 4v^4\right)^{c_2} (\operatorname{mod} \mathbb{Q}^{*2}) \\ \Rightarrow \qquad 3 & \equiv & \pm n^{c_1} \left(u^4 + 8u^2v^2 + 4v^4\right)^{c_2} (\operatorname{mod} \mathbb{Q}^{*2}). \end{array}$$

Upon comparing powers of 3 on both sides of the congruence we see, by Lemma 5.5(i), that $c_1 = 1$. Hence,

$$3 \quad \equiv \quad \pm n(\operatorname{mod} \mathbb{Q}^{*2}) \qquad \text{when } c_2 = 0 \tag{5.12}$$

and/or

$$3 \quad \equiv \quad \pm n \left(u^4 + 8u^2v^2 + 4v^4\right) (\operatorname{mod} \mathbb{Q}^{*2}) \qquad \text{when } c_2 = 1. \tag{5.13}$$

For congruence (5.12) we deduce that $2(u^4+2u^2v^2+4v^4)(u^4+8u^2v^2+4v^4)$ must be a square modulo $\mathbb{Q}$, since $n = 6(u^4+2u^2v^2+4v^4)(u^4+8u^2v^2+4v^4)$. However, by Lemma 5.3(iii) we know that $2(u^4+2u^2v^2+4v^4)(u^4+8u^2v^2+4v^4)$ is not a square modulo $\mathbb{Q}$. Similarly, in order for congruence (5.13) to hold we would require that $2(u^4 + 2u^2v^2 + 4v^4)$ be a square modulo $\mathbb{Q}$, which contradicts Lemma 5.3(iv). Altogether, this gives us that $\alpha(P_2) \not\equiv s(\operatorname{mod} \mathbb{Q}^{*2})$ for all $s \in S_1$ such that

$$\alpha(\Gamma) \supseteq S_2 \div < 1, n, (u^4 + 8u^2v^2 + 4v^4), 3 >,$$

where the elements of S_2 are generators for the subgroup of $\alpha(\Gamma)$ and $|S_2| = 16$.

Finally, consider

$$\alpha(P_3) = -(u^4 + 2u^2v^2 + 4v^4)(\operatorname{mod} \mathbb{Q}^{*2}).$$

In this case, we need to show that $\alpha(P_3) \not\equiv s(\operatorname{mod} \mathbb{Q}^{*2})$ for all $s \in S_2$. So, consider the case where the congruence holds then there would exist integers e_1, e_2 and e_3 with $e_1, e_2, e_3 \in \{0, 1\}$ such that

$$\begin{array}{rcl} \alpha(P_3) & \equiv & \pm 3^{e_1} n^{e_2} (u^4 + 8u^2v^2 + 4v^4)^{e_3} (\operatorname{mod} \mathbb{Q}^{*2}) \\ \Rightarrow -(u^4 + 2u^2v^2 + 4v^4) & \equiv & \pm 3^{e_1} n^{e_2} (u^4 + 8u^2v^2 + 4v^4)^{e_3} (\operatorname{mod} \mathbb{Q}^{*2}). \end{array}$$

Upon comparing powers of 2 on both sides of this congruence, as in the proof of Lemma 5.3, we deduce that

$$2^{2m} \parallel 3^{e_1} n^{e_2} (u^4 + 8u^2v^2 + 4v^4)^{e_3},$$

for some non-negative integer m. However, as determined in the proof of Lemma 5.3, there is an odd power of 2 exactly dividing n, such that e_2 must be 0. Therefore,

$$-(u^4 + 2u^2v^2 + 4v^4) \equiv \pm 3^{e_1} (u^4 + 8u^2v^2 + 4v^4)^{e_3} (\operatorname{mod} \mathbb{Q}^{*2}). \tag{5.14}$$

Comparing powers of 3 on both sides of (5.14) implies that $e_1 = 0$, by Lemma 5.5. So, either

$$-(u^4 + 2u^2v^2 + 4v^4) \equiv \pm 1 (\operatorname{mod} \mathbb{Q}^{*2}) \qquad \text{when } e_3 = 0 \tag{5.15}$$

and/or

$$-(u^4+2u^2v^2+4v^4) \equiv \pm(u^4+8u^2v^2+4v^4)(\operatorname{mod} \mathbb{Q}^{*2}) \quad \text{when } e_3 = 1. \tag{5.16}$$

For congruence (5.15) we deduce that $-(u^4+2u^2v^2+4v^4)$ must be a square modulo $\mathbb{Q}$. However, by Lemma 5.4(i) we know that $-(u^4 + 2u^2v^2 + 4v^4)$ is not a square modulo $\mathbb{Q}$. Similarly, in order for congruence (5.16) to hold we would require that $(u^4 + 2u^2v^2 + 4v^4)(u^4 + 8u^2v^2 + 4v^4)$ be a square modulo $\mathbb{Q}$, which is contradicted by Lemma 5.6. Altogether, this gives us that $\alpha(P_3) \not\equiv s (\operatorname{mod} \mathbb{Q}^{*2})$ for all $s \in S_2$ such that

$$\alpha(\Gamma) \supseteq S_2 \cup \left\{-(u^4 + 2u^2v^2 + 4v^4)\right\},$$

which contains at least 17 elements. Then since $|\alpha(\Gamma)|$ must be a power of 2 we have that $|\alpha(\Gamma)| \geq 32$, which is enough to show that the rank of $y^2 = x^3 - n^2x$ is at least 3.

□

Chapter 6

The Distribution of Congruent Numbers

Previously, it has been shown that every congruence class modulo eight contains infinitely many congruent numbers [Cha06]. That is to say, modulo 8 there exist infinitely many positive integers n such that the rank of the associated elliptic curve, $y^2 = x^3 - n^2x$, is at least 1. In general, it has been shown that every congruence class modulo m contains infinitely many congruent numbers for any integer m greater than 1 [Ben02]. The goal of this chapter is to prove a similar result involving congruent numbers where the rank of the associated elliptic curve is at least 2.

6.1 Rank Two Results

We begin by presenting the main theorem that will be proved in Section 6.2.

Theorem 6.1. [JS10] *If $m > 1$ is an integer then any congruence class modulo m contains infinitely many congruent numbers n, inequivalent modulo squares, such that the rank of $y^2 = x(x^2 - n^2)$ is greater than or equal to* 2*.*

We note that in Theorem 6.1, n is any positive integer not just a square-free integer. Before we prove Theorem 6.1 we need to recall the following theorem, that was conjectured by Mordell and then later proved by Faltings in 1983, where the term genus is a well-defined quantity associated with any algebraic curve [Hus04].

Theorem 6.2. [Hus04, Remark 6.4] [Faltings Theorem] *Let E be a non-singular curve (i.e. all the roots are distinct) of genus strictly greater than* 1*. Then the set $E(\mathbb{Q})$ of rational points on E is finite.*

Proof. See [Fal83].

□

We also need to prove the following lemma.

Lemma 6.3. [JS10] *Let $t \notin \{0, -1, -1/3\}$ be a rational number and define $f(t)$ by*

$$f(t) = t(t+1)(3t+1)(9t^4 + 24t^3 + 26t^2 + 8t + 1). \tag{6.1}$$

Then the elliptic curve

$$y^2 = x^3 - f(t)^2 x \tag{6.2}$$

has rank greater than or equal to 2, for all but finitely many values of t.

Proof. Given a rational number $t \neq 0, -1, -1/3$ let r be the rank of the elliptic curve

$$y^2 = x^3 - f(t)^2 x, \tag{6.3}$$

where $f(t)$ is as described in Equation (6.1). As in Chapter 4, let Γ be the group of rational points on the elliptic curve $y^2 = x^3 - f(t)^2 x$ and let $\overline{\Gamma}$ be the group of rational point on the elliptic curve $y^2 = x^3 + 4f(t)^2 x$. Then we need to find as many elements of $\alpha(\Gamma)$ and $\overline{\alpha}(\overline{\Gamma})$ where

$$\alpha(P) = \begin{cases} 1 (\operatorname{mod} \mathbb{Q}^{*2}), & \text{for } P = \mathcal{O}, \\ b (\operatorname{mod} \mathbb{Q}^{*2}), & \text{for } P = (0,0), \\ x (\operatorname{mod} \mathbb{Q}^{*2}), & \text{for } P = (x,y) \end{cases}$$

and

$$\overline{\alpha}(P) = \begin{cases} 1 (\operatorname{mod} \mathbb{Q}^{*2}), & \text{for } P = \mathcal{O}, \\ \overline{b} (\operatorname{mod} \mathbb{Q}^{*2}), & \text{for } P = (0,0), \\ x (\operatorname{mod} \mathbb{Q}^{*2}), & \text{for } P = (x,y). \end{cases}$$

Using the 2-descent method, as described in Chapter 4, we need to show that $2^r \geq 4$, since this would imply that the rank of $y^2 = x^3 - f(t)^2 x$ is at least 2. More specifically, since

$$2^r = \frac{|\alpha(\Gamma)| \cdot |\overline{\alpha}(\overline{\Gamma})|}{4}$$

we will show that $|\alpha(\Gamma)| \geq 8$ and $|\overline{\alpha}(\overline{\Gamma})| \geq 2$.

To start, recall that $\alpha(\Gamma)$ contains 1 and $b (\operatorname{mod} \mathbb{Q}^{*2})$, and for $b = b_1 b_2$ $\alpha(\Gamma)$ also contains $b_1 (\operatorname{mod} \mathbb{Q}^{*2})$ when the equation

$$N^2 = b_1 M^4 + a M^2 e^2 + b_2 e^4$$

has a solution with $M \neq 0$. In our case $b = -f(t)^2$ such that $1, -1 \in \alpha(\Gamma)$ by definition, since $-f(t)^2 \equiv -1 (\operatorname{mod} \mathbb{Q}^{*2})$. Then we need to only consider $b_1 = f(t), -f(t)$ plus all other divisors of $f(t)$.

Now, for $b_1 = f(t)$ and $b_1 = -f(t)$ consider the following equations:

(i) $N^2 = f(t)M^4 - f(t)e^4$

(ii) $N^2 = -f(t)M^4 + f(t)e^4$.

Clearly, the solution $(N, M, e) = (0, 1, 1)$ satisfies both of the above equations. It remains to show that $\pm f(t)$ is not a square in $\mathbb{Q}$. So, consider

$$Y^2 = \pm f(t) = \pm t(t+1)(3t+1)(9t^4 + 24t^3 + 26t^2 + 8t + 1). \tag{6.4}$$

Using the MAPLE$^{\text{TM}}$ code in Appendix A we find that Equation (6.4) is a genus 3 curve such that by Theorem 6.2 there are only finitely many solutions. Therefore, except for finitely many t values, we have

$$\alpha(\Gamma) \supseteq \{1, -1, f(t), -f(t)\}.$$

To find another element of $\alpha(\Gamma)$ we consider the following non-torsion point $P_1 = (x_1, y_1)$, that satisfies $y^2 = x^3 - f(t)^2 x$, where

$$\begin{aligned} x_1 &= -\frac{4t^2(t+1)^2(3t+1)^2(9t^4+24t^3+26t^2+8t+1)}{(3t^2+2t+1)^2} \\ y_1 &= \frac{2t^2(t+1)^2(3t+1)^2(3t^2-1)(9t^4+24t^3+26t^2+8t+1)^2}{(1+2t+3t^2)^3}. \end{aligned}$$

It remains to show that P_1 is distinct modulo $\mathbb{Q}^{*2}$, in $\alpha(\Gamma)$. So, consider

$$\alpha(P_1) \equiv -(9t^4 + 24t^3 + 26t^2 + 8t + 1)(\operatorname{mod} \mathbb{Q}^{*2}).$$

Then clearly P_1 is not congruent to ± 1 or $\pm f(t)$ modulo $\mathbb{Q}^{*2}$ as long as $\alpha(P_1)$ is not a square itself. However, if $\alpha(P_1)$ is a square in $\mathbb{Q}$ then we would have

$$Y^2 = \pm(9t^4 + 24t^3 + 26t^2 + 8t + 1). \tag{6.5}$$

Now, we need to only consider the positive case of (6.5), since the negative case yields no rational solutions for all rational values of t. So, consider

$$Y^2 = (9t^4 + 24t^3 + 26t^2 + 8t + 1),$$

which using the MAPLE$^{\text{TM}}$ code in Appendix A we find is bi-rationally equivalent to

$$Y^2 = t^3 - 5616t + 120960. \tag{6.6}$$

Using the MAGMA code in Appendix B we find that the rank of (6.6) is zero. Therefore, by definition, we have that there are only finitely many points that satisfy (6.6). This in turn gives us that, except for finitely many t values,

$$\begin{aligned}\alpha(\Gamma) \supseteq \quad & \{1, -1, f(t), -f(t), (9t^4 + 24t^3 + 26t^2 + 8t + 1), \\ & \qquad\qquad -(9t^4 + 24t^3 + 26t^2 + 8t + 1)\}.\end{aligned}$$

Then since $|\alpha(\Gamma)|$ must be a power of 2 we have that $|\alpha(\Gamma)| \geq 8$.

Next consider $b = 4f(t)^2$ such that $1 \in \overline{\alpha}(\overline{\Gamma})$ by definition. Then we need to only consider $b_1 = 4f(t), -4f(t)$, as well as the other divisors of $4f(t)$. We start with the following non-torsion point, $P_2 = (x_2, y_2)$, that satisfies $y^2 = x^3 + 4f(t)^2x$,

$$(x_2, y_2) = ((4t^2(9t^4 + 24t^3 + 26t^2 + 8t + 1), 4t^2(9t^4 + 24t^3 + 26t^2 + 8t + 1)^2).$$

It remains to show that $\overline{\alpha}(P_2)$ is not a square in $\mathbb{Q}$. So, consider

$$\overline{\alpha}(P_2) \equiv (9t^4 + 24t^3 + 26t^2 + 8t + 1)(\operatorname{mod} \mathbb{Q}^{*2}).$$

This, however, is the same as $-\alpha(P_1)$ which we already showed was a square in $\mathbb{Q}^{*2}$ for only finitely many rational t values. Hence,

$$\overline{\alpha}(\overline{\Gamma}) \quad \supseteq \quad \left\{1, (9t^4 + 24t^3 + 26t^2 + 8t + 1)\right\}$$

such that $|\overline{\alpha}(\overline{\Gamma})| \geq 2$. Altogether, we have shown that the rank of

$$y^2 = x^3 - f(t)^2x$$

is at least 2, for finitely many rational t values, since

$$\begin{aligned} 2^r &= \frac{|\alpha(\Gamma)| \cdot |\overline{\alpha}(\overline{\Gamma})|}{4} \\ &\geq \frac{8 \cdot 2}{4} \\ &= 4. \end{aligned}$$

□

6.2 Proof of the Main Theorem

We are now ready to prove Theorem 6.1.

Proof. Let m be a positive integer grater than 1. Then we need to show that every congruence class modulo m contains infinitely many congruent numbers n, inequivalent modulo squares, such that the associated elliptic curve, $y^2 = x^3 - n^2x$, has rank at least 2.

So, consider the integer $a \in \{1, 2, \ldots, m\}$, which is a representative of a congruence class modulo m. Then we need to show that there exist infinitely many positive integers n such that $n \equiv a (\operatorname{mod} m)$, the rank of the associated elliptic curve, $y^2 = x^3 - n^2x$, is at least 2 and the n's are inequivalent modulo squares. To do this we define the integer n to be

$$n \doteqdot \frac{f(am^2x^2)}{m^2x^2}, \tag{6.7}$$

where f is as defined in (6.1) and $x = 1, 2, \ldots$. So,

$$\begin{aligned} n = \quad & a(am^2x^2+1)(3am^2x^2+1)(9(am^2x^2)^4 \\ & +24(am^2x^2)^3 + 26(am^2x^2)^2 + 8am^2x^2 + 1), \end{aligned}$$

which is clearly a positive integer greater than zero and clearly $n \equiv a (\operatorname{mod} m)$. Moreover, by scaling Lemma 6.3 we have that the rank of $y^2 = x^3 - n^2x$ is at least 2, which also implies that n is a congruent number by Lemma 3.4. So far, since a and m are arbitrary and $x = 1, 2, \ldots$ we have shown that there exist infinitely many congruent numbers n in each congruence class modulo m such that the associated elliptic curve has rank at least 2. It remains to show that there exist infinitely many n's that are inequivalent modulo squares.

So, by way of contradiction assume that there exists a finite set of nonzero rational numbers d_i where $i = 1, \ldots k$ that are inequivalent modulo squares such that for each value of x in (6.7) we have

$$\frac{f(am^2x^2)}{m^2x^2} = d_iY^2, \tag{6.8}$$

where Y is a rational number dependent on x (i.e. there are only finitely many n's that are incongruent modulo squares). However, since there are an infinite number of distinct x values this would imply that there exists an infinite set of distinct points on the set of algebraic curves defined in (6.8). Using the MAPLE$^{\text{TM}}$ code in Appendix A we find that the algebraic curves defined in (6.8) have genus 5, of which we know by Theorem 6.2 that for each d_i there are only finitely many points satisfying each equation. Therefore, there must exist infinitely many numbers n that are inequivalent modulo squares.

Altogether, we have that there exist infinitely many congruent numbers n, inequivalent modulo squares, in each congruence class modulo m such that the associated elliptic curve has rank at least 2.

$\square$

Chapter 7

Future Work

Future work in this area would involve congruent numbers, elliptic curves or congruent number elliptic curves.

In the field of congruent numbers there are several topics that people may find interesting. For instance, one might look at finding another equivalent definition for a congruent number, as in Theorem 2.2. As we saw in Chapter **??** the more we know about congruent numbers the closer we are to solving the congruent number problem. The definition of a congruent number involving elliptic curves has brought us significantly closer to solving the congruent number problem and without this discovery we may not know nearly as much about congruent numbers [Cip09].

Another interesting topic of consideration would be to find more families of congruent numbers, similar to Chapter 2 Section 2.2. One might also be interested in looking closer at the statistical distribution of congruent numbers, as Rubinstein does in Chapter 1.

Specifically, given the results found in this thesis one might try to prove that for an integer $m > 1$ any congruence class modulo m contains infinitely many congruent numbers n, inequivalent modulo squares, such that the rank of $y^2 = x(x^2 - n^2)$ is greater than or equal to 3. Suffice it to say, there are still many open questions surrounding congruent numbers making this field of study interesting and beneficial to any inquisitive person.

When discussing elliptic curves it is important to remember that we do not necessarily need to talk about congruent number elliptic curves. A lot of work has been done with elliptic curves in general, however there are still some open problems surrounding this topic, including the BSD conjecture [Cip09]. The BSD conjecture is widely believed to be true and would provide significant results, including the verification of Tunnell's Theorem [Hem06].

Now for some future work involving congruent number elliptic curves. Based on the results found in Chapter 5 one might be interested in finding more families of congruent number elliptic curves with moderate rank, as well as individual congruent number elliptic curves with significant rank. Currently, the highest known rank of a congruent number elliptic curve is only 7 but it would be interesting to find higher ranks and possibly work with those individual curves to find families of congruent number elliptic curves with equivalent rank [DJS09].

In closing, I would like to say that the study of congruent numbers and congruent number elliptic curves is significant to many researchers for the simple reason that they are interesting, and that there are still a lot of unanswered questions [Cip09]. I thoroughly enjoyed working with congruent numbers and congruent number elliptic curves, and I look forward to continuing my work in this area.

Bibliography

[AC74] R. Alter and T. B. Curtz. A note on congruent numbers. *Math. Comp.*, 28(125):303–305, 1974. → pages 2, 7, 8, 12, 13, 14, 15, 16

[Alt80] R. Alter. The congruent number problem. *Amer. Math. Monthly*, 87:43–45, 1980. → pages 2, 7, 8

[Ben02] M. Bennett. Lucas' square pyramid problem revisited. *Acta Arith.*, 105:341–347, 2002. → pages 7, 8, 22, 40

[BM90] A. Brumer and O. McGuinness. The behavior of the mordell-weil group of elliptic curves. *Bull. Amer. Math. Soc. (N.S.)*, 23(2):375–382, 1990. → pages 29

[Cha98] V. Chandrasekar. The congruent number problem. *Resonance*, 3(8):33–45, 1998. → pages 2, 10

[Cha06] J. Chahal. Congruent numbers and elliptic curves. *Amer. Math. Monthly*, 113(4):308–317, 2006. → pages 2, 7, 8, 21, 22, 23, 25, 40

[Cip09] B. Cipra. Congruent numbers. http://bit-player.org/2009/congruent-numbers, 2009. → pages 2, 3, 7, 8, 12, 46, 47

[Coa05] J. Coates. Congruent number problem. *Q. J. Pure Appl. Math.*, 1(1):14–27, 2005. → pages 2, 8

[Dic20] Leonard Eugene Dickson. *History of the Theory of Numbers*, volume 2. Carnegie Institute of Washington, 1920. → pages 10, 16, 17

[DJS09] A. Dujella, A. Janfada, and S. Salami. A search for high rank congruent number elliptic curves. *J. Integer Seq.*, 12, 2009. → pages 2, 8, 22, 29, 47

[Fal83] G. Faltings. Endlichkeitssätze für abelsche varietäten über zahlkörpern. *Invent. Math.*, 73(3):349–366, 1983. → pages 40

[Fra03] J. B. Fraleigh. *A First Course in Abstract Algebra*. Addison Wesley, Boston, seventh edition, 2003. → pages 5

[God78] H. Godwin. A note on congruent numbers. *Math. Comp.*, 32(141):293–295, 1978. → pages 7, 8

[Hem06] B. Hemenway. On recognizing congruent primes. Master's thesis, Simon Fraser University, 2006. → pages 2, 3, 7, 8, 12, 21, 22, 23, 46

[Hus04] D. Husemöller. *Elliptic Curves*. Springer, New York, second edition, 2004. → pages 20, 21, 22, 40

[JS] J. Johnstone and B. Spearman. Congruent number elliptic curves with rank at least 3. To appear in Canad. Math. Bull. → pages 29, 30, 32, 33, 34, 35

[JS10] J. Johnstone and B. Spearman. On the distribution of congruent numbers. *Proc. Japan Acad. Ser. A Math. Sci.*, 86(5):89–90, 2010. → pages 40, 41

[Kob92] N. Koblitz. *Introduction to Elliptic Curves and Modular Forms*. Springer, New York, 1992. → pages 2, 3, 7, 8, 12, 22, 23

[Kra86] G. Kramarz. All congruent numbers less than 2000. *Math. Ann.*, 273(2):337–340, 1986. → pages 2, 3, 7, 8, 22

[Nem98] F. Nemenzo. All congruent numbers less than 40000. *Proc. Japan Acad. Ser. A Math. Sci.*, 74(1):29–31, 1998. → pages 8, 22

[NW93] K. Noda and H. Wada. All congruent numbers less than 10000. *Proc. Japan Acad. Ser. A Math. Sci.*, 69(6):175–178, 1993. → pages 3, 8, 22

[Ros05] K. Rosen. *Elementary Number Theory and Its Applications*. Addison Wesley, Boston, fifth edition, 2005. → pages 1, 2, 8, 10, 16, 17

[Sil86] J.H. Silverman. *The Arithmetic of Elliptic Curves*. Springer, New York, 1986. → pages 20, 21, 22, 25, 26

[ST93] J.H. Silverman and J. Tate. *Rational Points on Elliptic Curves*. Springer, New York, second edition, 1993. → pages 18, 20, 21, 22, 24, 25, 26

[SZ03] S. Schmitt and H. Zimmer. *Elliptic Curves.* Walter de Gruyter, Berlin, 2003. → pages 20, 21, 22

[tFE] Wikipedia the Free Encyclopedia. Birch and swinnerton-dyer conjecture. http://en.wikipedia.org/wiki/Birch_and_Swinnerton-Dyer_conjecture. → pages 21

[Tun83] J. Tunnell. A classical diophantine problem and modular forms of weight 3/2. *Invent. Math.*, 72:323–334, 1983. → pages 2, 3, 7, 8

[Wal05] P.G. Walsh. Squares in lucas sequences with rational roots. *Integers*, 5(A15):1–8, 2005. → pages 34

Appendix A

MAPLE Code

The calculations in this section were executed using MAPLE 12 where > is used to reference MAPLE input and center text is used to reference MAPLE output.

A.1 Worked Example Calculations from Section4.2

Finding the rank of $y^2 = x(x^2 - 23^2)$.
$> e3_\Gamma := N^2 + 23M^4 - 23e^4$:
$> seq(seq(isolve(e3_\Gamma]), M = 1..10), e = 1..10)$;

$$\{N = 0\}, \{N = 0\}, \{N = 0\}, \{N = 0\}, \{N = 0\},$$
$$\{N = 0\}, \{N = 0\}, \{N = 0\}, \{N = 0\}, \{N = 0\}$$

$> soln := subs(N = 0, e3_\Gamma])$;

$$soln := 23\,M^4 - 23\,e^4$$

$> seq(isolve(soln), e = 1..10)$;

$$\{M = 1\}, \{M = -1\}, \{M = 2\}, \{M = -2\}, \{M = 3\},$$
$$\{M = -3\}, \{M = -4\}, \{M = 4\}, \{M = -5\}, \{M = 5\},$$
$$\{M = -6\}, \{M = 6\}, \{M = -7\}, \{M = 7\}, \{M = -8\},$$
$$\{M = 8\}, \{M = 9\}, \{M = -9\}, \{M = -10\}, \{M = 10\}$$

Hence there exists a *soln* satisfying the gcd conditions, namely $(0, 1, 1)$.

```
> with(numtheory):
> divisors(2116);
```

$$\{1, 2, 4, 23, 46, 92, 529, 1058, 2116\}$$

$> e3_2 := N^2 - 2M^4 - 1058e^4 :$
$> seq(seq(isolve(e3_2), M = 1..50), e = 1..50);$

$$\{N = -410\}\,, \{N = 410\}\,, \{N = -1640\}\,, \{N = 1640\}\,, \{N = -9430\}\,,$$

$$\{N = 9430\}\,, \{N = -37720\}\,, \{N = 37720\}$$

$> soln_1 := subs(N = 410, e3_2);$

$$soln_1 := 168100 - 2\,M^4 - 1058\,e^4$$

$> seq(isolve(soln_1), e = 1..10);$

$$\{M = -17\}\,, \{M = 17\}$$

$> factor(subs(M = 17, soln_1));$

$$-1058\,(e-1)\,(e+1)\left(e^2+1\right)$$

Hence, the solution $(410, 17, 1)$ satisfies the equation and the gcd conditions.

A.2 Chapter 5 Calculations

Finding the resultants for the factors defined in Lemma 5.6.
$> f := u^4 + 2u^2v^2 + 4v^4 :$
$> g := u^4 + 8u^2v^2 + 4v^4 :$
$> resultant(f, g, u);$

$$20736v^{16}$$

$> resultant(f, g, v);$

$$20736u^{16}$$

$> ifactor(20736);$

$$(2)^8(3)^4$$

Converting $w^2 = t^4 + 14t^2 + 4$ to $y^2 = x^3 - 6588x + 39312$ in the proof of Lemma 5.7.
$>\ \ with(algcurves) :$
$> f := t^4 + 14t^2 + 4 - w^2 :$
$> genus(f, t, w);$

$$1$$

$> newf := expand(subs(t = 3t, f));$

$$81t^4 + 126t^2 + 4 - w^2$$

$> sol := Weierstrassform(newf, t, w, x, y);$

$$\Big[x^3 - 6588\,x + y^2 - 39312,$$

$$\tfrac{-2(21\,t^2+4-2\,w)}{t^2},\ \tfrac{-8(4+63\,t^2-2\,w)}{t^3},\ \tfrac{-4y}{468+84\,x+x^2},\ \tfrac{-1}{2}\ \tfrac{-30096-672\,x+4\,x^2}{468+84\,x+x^2}\Big]$$

$> subs(x = -x, sol[1]);$

$$-x^3 + 6588x + y^2 - 39312$$

Similarly, we can convert $Y^2 = (9t^4 + 24t^3 + 26t^2 + 8t + 1)$ to $Y^2 = t^3 - 5616t + 120960$ by first scaling t by $1/3$ and then applying the $Weierstrassform$ command in MAPLE$^{\mathrm{TM}}$.

A.3 Chapter 6 Calculations

Genus calculations corresponding to Equation (6.4) and Equation (6.8, respectively.
$> with(algcurves);$
$> genus(x(x + 1)(3x + 1)(9x^4 + 24x^3 + 26x^2 + 8x + 1) + y^2, x, y);$

$$3$$

$> genus(\frac{dy^2-am^2x^2(am^2x^2+1)(3am^2x^2+1)(9(am^2x^2)^4+24(am^2x^2)^3+26(am^2x^2)^2+8am^2x^2+1)}{(m^2x^2)}, x, y);$

$$5$$

Appendix B

MAGMA Code

The calculations in this section were done using an online trial version of MAGMA Version 2.16-10, which can be found at

`http://magma.maths.usyd.edu.au/calc/`.

B.1 Elliptic Curve Calculations

Calculating the rank of the elliptic curve $y^2 = x^3 - 25x$ defined on page 22.

```
Input:
E := EllipticCurve([−25, 0]);
MordellWeilGroup(E);
Rank(E);
Output:
Abelian Group isomorphic to ℤ/2 + ℤ/2 + ℤ
Defined on 3 generators
Relations:
2 * $.1 = 0
2 * $.2 = 0
1
```

Calculating the rank of the elliptic curve $y^2 = x^3 - 6^2x$ in Example 3.5.

```
Input:
E := EllipticCurve([−6^2, 0]);
Rank(E);
Output:
1
```

Calculating the rank of the elliptic curve $y^2 = x^3 - 42486^2x$ in Example 5.2.

```
Input:
E := EllipticCurve([−42486^2, 0]);
Rank(E);
Output:
```

```
Warning: rank computed (3) is only a lower bound
(It may still be correct, though)
3
```

Calculating the rank of $x^3 + 2x^2 + 4x = y_1^2$ and $x^3 + 8x^2 + 4x = y_2^2$ in the proof of Lemma 5.4.

Input:

```
E1 := EllipticCurve([0, 2, 0, 4, 0]);
Rank(E1);
E2 := EllipticCurve([0, 8, 0, 4, 0]);
Rank(E2);
```

Output:

```
0
0
```

Finding the rational points on $x^3 + 2x^2 + 4x = y_1^2$ and $x^3 + 8x^2 + 4x = y_2^2$ in the proof of Lemma 5.4.

Input:

```
E1 := EllipticCurve([0, 2, 0, 4, 0]);
MordellWeilGroup(E1);
RationalPoints(E1 : Bound := 1000);
E2 := EllipticCurve([0, 8, 0, 4, 0]);
MordellWeilGroup(E2);
RationalPoints(E2 : Bound := 1000);
```

Output:

```
Abelian Group isomorphic to ℤ/2
Defined on 1 generator
Relations:
2 * $.1 = 0
{@(0 : 1 : 0), (0 : 0 : 1)@}
Abelian Group isomorphic to ℤ/4
Defined on 1 generator
Relations:
4 * $.1 = 0
{@(0 : 1 : 0), (0 : 0 : 1), (−2 : 4 : 1), (−2 : −4 : 1)@}
```

Note that the torsion subgroup of $E1$ is isomorphic to $\mathbb{Z}/2$ which implies that there are only 2 points of finite order, namely the point at infinity and $(0, 0)$. Also note that the torsion subgroup of $E2$ is isomorphic to $\mathbb{Z}/4$ which implies that there are only 4 points of finite order, namely the point at infinity, $(0, 0)$, $(-2, 4)$ and $(-2, -4)$.

Calculating the rank of the elliptic curve $Y^2 = X^3 - 6588X + 39312$ in the proof of Lemma 5.7.

Input:

```
E := EllipticCurve([0,0,0,-6588,39312]);
Rank(E);
```

Output:

```
1
```

Calculating the rank of the elliptic curve $Y^2 = t^3 - 5616t + 120960$ in the proof of Lemma 6.3.

Input:

```
E := EllipticCurve([0,0,0,-5616,120960]);
Rank(E);
```

Output:

```
0
```