On Recognizing Congruent Primes

by

Brett Hemenway

B.Sc., Brown University 2004

A THESIS SUBMITTED IN PARTIAL FULFILLMENT
OF THE REQUIREMENTS FOR THE DEGREE OF
MASTER OF SCIENCE
IN THE DEPARTMENT
OF
MATHEMATICS

SIMON FRASER UNIVERSITY
Fall 2006

APPROVAL

Name: Brett Hemenway

Degree: Master of Science

Title of thesis: On Recognizing Congruent Primes

Examining Committee: Dr. Jason Bell
Chair

Dr. Nils Bruin
Senior Supervisor

Dr. Peter Borwein
Supervisor

Dr. Stephen Choi
Supervisor

Dr. Imin Chen
Internal/External Examiner

Date Approved: September 12th, 2006

Abstract

An integer n is called "congruent" if it corresponds to the area of a right triangle with three rational sides. The problem of classifying congruent numbers has an extensive history, and is as yet unresolved. The most promising approach to this problem utilizes elliptic curves. In this thesis we explicitly lay out the correspondence between the congruence of a number n and the rank of the elliptic curve $y^2 = x^3 - n^2x$. By performing two-descents on this curve and isogenous curves for $n = p$ a prime, we are able to obtain a simple and unified proof of the majority of the known results concerning the congruence of primes. Finally, by calculating the equations for homogeneous spaces associated to the curve when $p \equiv 1 \mod 8$, we position the problem for future analysis.

Acknowledgments

I would like to thank my entire thesis committee. In particular, thanks to Peter Borwein for welcoming me into the SFU mathematical community, for making my time in Canada possible, and for his continued guidance throughout my time at SFU.

Thanks also to Nils Bruin for introducing me to the study of elliptic curves, for helping me navigate this project, and for reading many many drafts of this thesis. His constant encouragement, feedback and support has made him a wonderful advisor.

Dedication

To Emily.

Contents

Chapter 1

Introduction

1.1 Congruent Numbers

A positive rational number $n \in \mathbb{Q}$ is said to be a *Congruent Number* if it is the area of a right triangle with rational sides, i.e. if there are rational numbers a, b, c such that

$$\begin{cases} a^2 + b^2 &= c^2 \\ \frac{1}{2}ab &= n. \end{cases} \tag{1.1}$$

If n is a congruent number, then nr^2 is also congruent for any $r \in \mathbb{Q}$, since nr^2 is the area of the triangle with sides ra, rb, rc. Thus whether a number is congruent is determined solely by its residue class in the group $\mathbb{Q}^*/(\mathbb{Q}^*)^2$. With this in mind, when searching for congruent numbers we restrict our attention to square free integers. The question of determining which numbers are congruent is known as the Congruent Number Problem, and while the statement is completely elementary, this problem has been investigated by mathematicians for over one thousand years (see [10]) without leading to a complete solution. By performing elementary transformations on the equations (1.1), the problem can be formulated in many different ways. The earliest known reference the Congruent Number Problem is from A.D. 972 (see [10]), and states the problem in another form. A rational number n is said to be congruent if there exists a rational number x such that $x^2 + n$ and $x^2 - n$ are both

squares. This is also the formulation that Leonardo Pisano (Fibonacci) used to show that 5 is a congruent number in 1220 [10]. This formulation gives some insight into the name, since the three squares, x^2-n, x^2, x^2+n are congruent modulo n. The two definitions of a Congruent Number are easily seen to be equivalent by the maps

$$\begin{array}{ccccccccc} (& a & , & b & , & c &) & \mapsto & c/2 \\ (& \sqrt{x^2+n}-\sqrt{x^2-n} & , & \sqrt{x^2+n}+\sqrt{x^2-n} & , & 2x &) & \leftarrow & x. \end{array}$$

For most of this thesis we will be using a third characterization of congruent numbers, one relating to rational solutions to a cubic equation.

A square-free natural number n is a congruent number if we can simultaneously solve two equations over the rationals

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

which means

$$\frac{(a \pm b)^2}{4} = \left(\frac{c}{2}\right)^2 \pm n.$$

Then setting $x = \left(\frac{c}{2}\right)^2$ and $y = (a^2-b^2)\frac{c}{8}$ gives a solution to the cubic equation

$$E : y^2 = x^3 - n^2 x. \tag{1.2}$$

We will carefully examine the curve give by equation 1.2 in the case when n is prime to determine whether n is congruent.

1.2 Known Results

We now give a brief review of what is currently known about the Congruent Number Problem. Assuming the Birch and Swinnerton-Dyer Conjecture [4], the problem was essentially solved by Jerold B. Tunnell in 1983.

Tunnell's Theorem. *Define*

$$A_n = \#\{x, y, z \in \mathbb{Z} | n = 2x^2 + y^2 + 32z^2\}$$
$$B_n = \#\{x, y, z \in \mathbb{Z} | n = 2x^2 + y^2 + 8z^2\}$$
$$C_n = \#\{x, y, z \in \mathbb{Z} | n = 4x^2 + 2y^2 + 64z^2\}$$
$$D_n = \#\{x, y, z \in \mathbb{Z} | n = 8x^2 + 2y^2 + 16z^2\}$$

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 holds for curves of the form $y^2 = x^3 - n^2x$ then, conversely, these equalities imply n is a congruent number.

Proof. See [34], or [20] Chapter IV section 4. □

Currently this provides a method for showing certain numbers are not congruent, and assuming the Birch and Swinnerton-Dyer Conjecture this would provide a fairly efficient method for determining whether a given number is congruent, since counting solutions to these equations can be done easily. We will not go into details about the Birch and Swinnerton-Dyer conjecture, but it should be noted that it is widely believed to be true, and is one of the Clay Mathematics Institute's Millenium Prize Problems.

Much study has gone into Congruent Number Problem, not assuming the Birch and Swinnerton-Dyer Conjecture, and we will list the known results here. Let p_i and q_i denote distinct primes with $p_i \equiv q_i \equiv i \mod 8$ Then the following results are known

p_3 is *not* a congruent number	Genocchi, 1855 [13] and Tunnell, 1983 [34]
p_3q_3,$2p_5, p_5q_5$ are *not* congruent numbers	Genocchi [13] and Tunnell [34]
p_5, p_7 are congruent numbers	Monsky, 1990 [24]
$2p_7, 2p_3, p_3q_7, 2p_3q_5, 2p_5q_7$ are congruent numbers	Monsky, 1990 [24]

Overviews of progress made on the Congruent Number Problem can be found in [10], [14], [1], [8], [28] and [27].

In this thesis, we obtain upper bounds for the rank of the elliptic curve $y^2 = x^3 - n^2x$ using the method of 2-descent. In this way, we show that p_3 is not a congruent

number, p_5, p_7 are congruent numbers assuming the conjecture that $Ш(E/K)[2]$ is finite, and for p_1, if we decompose $p_1 = a^2+b^2$, then p_1 is not congruent if $(a+b)^2 \not\equiv 1 \mod 16$. This last result was stated by Bastien in 1915 [2], but a proof does not seem to have appeared in the literature until Tunnell's proof in [34]. Tunnell's proof comes as a consequence of Tunnell's Theorem, and hence his method is very different from the one presented here.

The case of when $p \equiv 3 \mod 8$ was the first to be resolved. In 1855 Angelo Genocchi showed that p_3 is not a congruent number. His paper predates much of the general machinery of elliptic curves, and his argument is fairly elementary. Nevertheless, Genocchi's method bears many similarities to the method of descent used in this thesis. To show that p_3 is not congruent, Genocchi shows that if p_3 were congruent, this would lead to an integral point on a quartic, then he shows that because -1 and 2 are not squares in $\mathbb{Z}/p_3\mathbb{Z}$, these quartics have no rational points. To illustrate his technique, we give an overview of his original argument in §1.3.

1.3 Genocchi's 1855 Argument

We now make a brief digression to give Genocchi's argument [13] that if p is a prime with $p \equiv 3 \mod 8$ then p is not a congruent number. Genocchi's paper is often cited, as it is one of the earliest demonstrations that an entire class of numbers is not congruent. Unfortunately, his paper has become very difficult to obtain. For its historical significance, as well as its ingenuity, we give a detailed account of his argument. The terminology has been updated, but the content of the proof remains the same.

Fibonacci gave the following characterization of congruent numbers. A number is congruent if it is one of the four numbers $a, b, a+b, a-b$ and the remaining three numbers are square. This is equivalent to the statement that n is congruent if there is a rational number x such that $x^2 \pm n$ are both square. Genocchi begins with Fibonacci's characterization, and considers four cases separately.

Throughout the proof, we will make use of the fact that all Pythagorean Triples

can be paramatrized as

$$(r^2 - s^2, 2rs, r^2 + s^2).$$

Suppose n is a congruent number then one of the following four cases holds.

Case 1:

$$a = nf^2, b = g^2, a + b = h^2, a - b = k^2.$$

Thus we have

$$a^2 - b^2 = h^2k^2, a^2 = b^2 + (hk)^2.$$

So b, hk, a is a Pythagorean Triple. Then parametrizing we have $a = r^2 + s^2$ and $b = r^2 - s^2$ or $b = 2rs$. This gives

$$g^2 = b = (r^2 - s^2) = (r - s)(r + s)$$

or

$$g^2 = b = 2rs.$$

In the first case, since r, s are relatively prime, we must have $r + s = \alpha^2$, $r - s = \beta^2$. This gives

$$\alpha^4 + \beta^4 = 2nf^2. \tag{1.3}$$

In the second case, we get

$$\alpha^4 + 4\beta^4 = nf^2. \tag{1.4}$$

Case 2:

$$a = f^2, b = g^2, a + b = h^2, a - b = nk^2.$$

Thus we have

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

Thus (f, g, h) is a pythagorean triple, so $(f, g) = (r^2 - s^2, 2rs)$ or $(f, g) = (2rs, r^2 - s^2)$. From the equation $f^2 - g^2 = nk^2$, we then obtain

$$(r^2 - s^2)^2 - (2rs)^2 = \pm nk^2.$$

Expanding gives

$$r^4 - 6r^2s^2 + s^4 = \pm nk^2. \tag{1.5}$$

Case 3:

$$a = f^2, b = g^2, a + b = nh^2, a - b = k^2.$$

Thus we have

$$k^2 + g^2 = f^2.$$

So parametrizing this pythagorean triple, we have $f = r^2 + s^2$ and $g = 2rs$ or $g = r^2 - s^2$, plugging into the equation

$$f^2 + g^2 = nh^2$$

gives

$$(r^2 + s^2)^2 + (2rs)^2 = nh^2$$

or

$$(r^2 + s^2)^2 + (r^2 - s^2)^2 = nh^2.$$

Thus

$$r^4 + 6r^2s^2 + s^4 = nh^2 \tag{1.6}$$

or

$$2r^4 + 2s^4 = nh^2. \tag{1.7}$$

Case 4:

$$a = f^2, b = ng^2, a + b = h^2, a - b = k^2.$$

Here, we are forced to use a different method since

$$f^2 + ng^2 = h^2$$

and

$$f^2 - ng^2 = k^2$$

tell us only that n is a congruent number. Going back to the definition of a congruent number, if n is congruent, we can find $x_1, x_2, x_3 \in \mathbb{Q}$ such that

$$x_2^2 - n = x_1^2, x_2^2 + n = x_3^2.$$

Clearing denominators we can find q such that $x_i = \frac{p_i}{q}$ where $p_i, q \in \mathbb{Z}$. Here, we assume that q is the smallest integer such that $p_1, p_2, p_3 \in \mathbb{Z}$. Thus we have the equations

$$p_2^2 - nq^2 = p_1^2, p_2^2 + nq^2 = p_3^2.$$

Since

$$p_3^2 - p_1^2 = 2nq^2,$$

we conclude that $p_1 \equiv p_3 \mod 2$, thus we can define *integers*

$$r_1 = \frac{p_1 + p_3}{2}, r_3 = \frac{p_3 - p_1}{2}.$$

This gives

$$p_2^2 = r_1^2 + r_3^2,$$

which is a Pythagorean Triple, so we can parametrize this as

$$p_2 = a^2 + b^2, r_1 = a^2 - b^2, r_3 = 2ab.$$

Now, we also have $nq^2 = 2r_1r_3$, so substituting our parametrization for r_1, r_3 we get

$$nq^2 = 4ab(a - b)(a + b).$$

Since n is congruent, we also know that we can find integers a, b such that three of the four integers $a, b, a + b, a - b$ are square and n divides fourth. Assuming we are not in one of the three previous cases, if n is prime we must have $n|b$, so

$$f^2 + ng^2 = h^2, f^2 - ng^2 = k^2.$$

Then, these equations give

$$nq^2 = 4f^2k^2ng^2(ng^2 + f^2).$$

So $ng^2 < nq^2$, but this contradicts the minimality of q. Thus we conclude that this case is impossible for n prime.

It remains to show that the first three cases are impossible. Genocchi does this by examining congruence conditions mod p. Gathering equations (1.3) - (1.7), and unifying notation, we have

$$2nf^2 = r^4 + r^4, \tag{1.8}$$
$$2nf^2 = r^4 + 4b^4, \tag{1.9}$$
$$\pm nf^2 = r^4 - 6r^2s^2 + s^4, \tag{1.10}$$
$$nf^2 = r^4 + 6r^2s^2 + s^4, \tag{1.11}$$
$$nf^2 = 2r^4 + 2s^4. \tag{1.12}$$

If $p \equiv 3 \mod 8$ and $p|n$, then taking remainders modulo p shows that Equations (1.8), (1.9), (1.12) are impossible since -1 is not a square mod p. To deal with equation (1.10), we notice that

$$r^4 - 6r^2s^2 + s^4 = (r^2 - 3s^2)^2 - 2(2s^2)^2$$
$$-r^4 + 6r^2s^2 - s^4 = (r^2 + s^2)^2 - 2(r^2 - s^2)^2,$$

and 2 is not a square mod p. Similarly for equation (1.11), we observe

$$r^4 + 6r^2s^2 + s^4 = (r^2 + s^2)^2 + (2rs)^2 = (r^2 + 3s^2)^2 - 2(2s^2)^2,$$

and it suffices to notice that either -1 or 2 is not a square mod p.

Thus if $p \equiv 3 \mod 8$, then p is not a congruent number.

Chapter 2

Elliptic Curves

2.1 Introduction

We will be looking for rational solutions (x, y) to the equation $E : y^2 = x^3 - n^2x$. This is an example of an elliptic curve. The theory of elliptic curves is well-developed, and before we begin analyzing the curve E, we review some of the general properties of elliptic curves that we will use.

2.2 Definition

Let $\mathbb{P}^2$ denote the projective plane. An elliptic curve is the locus of points in $\mathbb{P}^2$

$$E : Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3.$$

It is usually convenient to de-homogenize, i.e. change variables and let $x = X/Z$ and $y = Y/Z$. Then we have the equation

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

When the characteristic of the base field is not equal to 2 or 3, then we can make a change of variables resulting in the simpler form

$$E : y^2 = x^3 + ax + b.$$

We denote by $\mathbf{0}$ the point $[0:1:0]$ on E. Since this is the only point with $Z = 0$ on E, for convenience, we will often denote a point P on E with $P \neq \mathbf{0}$ simply as $P = (x, y)$, where this is shorthand for the point $P = (x : y : 1)$.

Recall that a function $f(x) = x^3+ax+b$ has a double root if and only if $4a^3+27b^2 = 0$. A curve given by the equation $y^2 = f(x)$ is called singular if $f(x)$ has a double root.

2.3 Finite Fields

An elliptic curve $E : y^2 = x^3 + ax + b$, is said to be defined over $\mathbb{Q}$ if $a, b \in \mathbb{Q}$. A point on E is called rational if its coordinates are rational numbers. When studying the rational points, it can be useful to examine the points in $\mathbb{F}_q$ for $q = p^f$, where $\mathbb{F}_q$ denotes the finite field with q elements. For the curve to remain nonsingular in $\mathbb{F}_q$, we need $-16(4a^3 + 27b^2) \neq 0 \in \mathbb{F}_q$ which means $p \nmid 2$ and $p \nmid 4a^3 + 27b^2$. Assuming this is the case, we denote the natural map

$$\begin{aligned} \mathbb{Z} &\to \mathbb{Z}/p\mathbb{Z} \hookrightarrow \mathbb{F}_q \\ x &\mapsto \bar{x}, \end{aligned}$$

for any rational point $(X : Y : Z)$ on E, we can choose X, Y, Z such that $X, Y, Z \in \mathbb{Z}$ and $\gcd(X, Y, Z) = 1$. Then we have a map

$$\begin{aligned} P &\mapsto \bar{P} \\ (X : Y : Z) &\mapsto (\bar{X} : \bar{Y} : \bar{Z}). \end{aligned}$$

Since $\gcd(X, Y, Z) = 1$, we cannot have $\bar{X} = \bar{Y} = \bar{Z} = 0$, thus $\bar{P}$ is a point in $\mathbb{P}^2(\mathbb{F}_q)$. We can sometimes (as in the proof of Theorem 1) use the finiteness of $\mathbb{P}^2(\mathbb{F}_q)$ to great advantage.

2.4 The Group Law

The set of rational points on an elliptic curve can be made into an abelian group, with $\mathbf{0}$ acting as the identity, and it is towards this group that we direct our further attentions.

For a more in depth discussion of the group law, see [29] III.2, [5] Chapter 7, or [18] Chapter 3.

We describe the group law geometrically. First, we need a lemma.

Lemma 1. *If $P = (X_1 : Y_1 : Z_1)$ and $Q = (X_2 : Y_2 : Z_2)$ are two rational points on the curve E, then the line L through P and Q intersects E in a third rational point, R.*

Proof. This is a direct consequence of Bézout's Theorem ([15] Theorem 18.3 or [16] Corollary I.7.8). □

This means that the line at infinity intersects E with multiplicity 3 at $\mathbf{0}$. The line through the point $\mathbf{0}$ and R intersects the curve E in a third point by lemma 1, and we call this third point of intersection $P + Q$ (see figure 2.1). This operation makes the rational points on E into an abelian group.

It is straightforward to check that

$$P + \mathbf{0} = P,$$
$$P + Q = Q + P.$$

Associativity can be checked directly, but the calculations are long. A verification using MAGMA can be found at [30]. We give a short argument for the associativity given in [5] Chapter 7. First, we note that three points P, Q, R are collinear if and only if there exists a linear form L_1 such that L_1 has zeros at P, Q, R. Thus if $\mathbf{0}, R, S$ are collinear, then there is a linear form L_2 with zeros at $\mathbf{0}, R, S$.

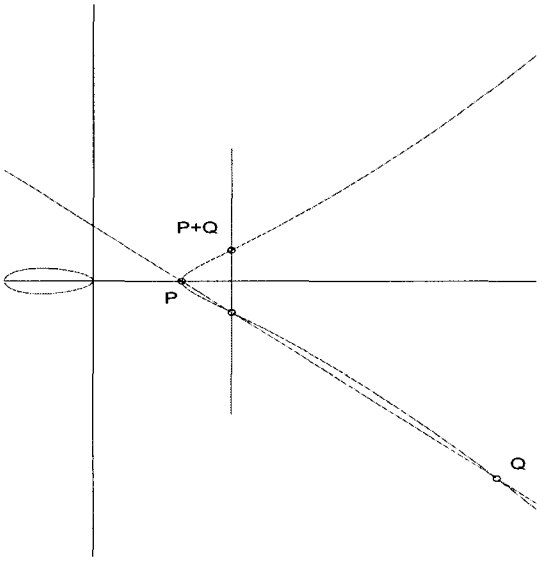

Figure 2.1: The addition law on the curve $y^2 = x^3 - 41^2x$.

Suppose the points P, Q, R are collinear and $\mathbf{0}, R, S$ are collinear, i.e. $P+Q = S$. Since P, Q, R are collinear there exists a linear form L_1, such that L_1 has zeros at P, Q, R. Similarly there exists a linear form L_2 with zeros at $\mathbf{0}, R, S$.

Thus the rational function $\frac{L_1}{L_2}$ is defined on the curve E and has zeros at P, Q and poles at $\mathbf{0}, S$. In fact, the converse holds as well: if there exists a rational function f with zeros at P, Q and poles at $\mathbf{0}, S$, then $P + Q = S$. With this characterization of the addition law, it becomes straightforward to see that associativity holds. The equation

$$X = (P + Q) + T,$$

is thus equivalent to the existence of a function with simple poles at P, Q, T a double

zero at $\mathbf{0}$, and a simple zero at X. But this is exactly the same as the function corresponding to the equation

$$X = P + (Q + T),$$

so we conclude that $(P + Q) + T = P + (Q + T)$. This characterization of will also be useful in our study of isogenies.

The group law can be given explicitly as functions on the coordinates of the points. As we will not have occasion to use the group law in its full generality, we will calculate only a few special cases here. We will be interested in curves of the form

$$E : y^2 = x^3 + a_4 x$$

Let $P = (x_0, y_0)$ be a point on E. This curve E is now symmetric about the x-axis. The line through P and $\mathbf{0}$ is vertical, so it intersects the curve again at the point $(x_0, -y_0)$. Thus $(x_0, -y_0) + (x_0, y_0) = \mathbf{0}$, because the line through $\mathbf{0}$ and $\mathbf{0}$ intersects at $\mathbf{0}$ with multiplicity 3. Thus we have

$$-P = (x_0, -y_0).$$

As is the case with any abelian group, we can consider the group E as a $\mathbb{Z}$-module under the action

$$[n]P = \underbrace{P + \ldots + P}_{n \text{ times}}$$

Let us calculate $2P$ for $P = (x_0, y_0)$ on the curve $E : y^2 = x^3 + ax + b$. The tangent at the point (x_0, y_0) has slope

$$\lambda = \frac{3x_0^2 + a}{2y_0}.$$

So the equation of the tangent line becomes

$$y = \lambda x + y_0 - \lambda x_0.$$

This intersects the curve at the point (x_1, y_1) where

$$\begin{aligned} x_1 &= \frac{1}{4}\frac{x_0^4 - 2ax_0^2 - 8bx_0 + a^2}{y_0^2} \\ y_1 &= \frac{1}{8}\frac{x_0^6 + 5ax_0^4 + 20bx_0^3 - 5a^3x_0^2 - 4abx_0 - a^3 - 8b^3}{y_0^3} \end{aligned} \tag{2.1}$$

2.5 The Structure of the Group

The group of rational points on an elliptic curve is clearly abelian, but we can say much more.

Mordell-Weil Theorem. *The group of rational points on an elliptic curve is finitely generated.*

Proof. See [29] Theorem 4.1, [5] Theorem 13.1 and [18] Theorem 7.4. □

Fundamental Theorem of Finitely Generated Abelian Groups. *Every finitely generated abelian group is the direct product of a finite torsion group and a number of copies of infinite cyclic groups (i.e. $\mathbb{Z}$).*

Proof. See [26] Theorem 10.20. □

We now know that the group $E(\mathbb{Q})$ can be decomposed as

$$E(\mathbb{Q}) \simeq E(\mathbb{Q})_{\text{tors}} \times \mathbb{Z}^r,$$

where the integer r is known as the *rank* of the curve. Thus to fully describe the group $E(\mathbb{Q})$, we only need to calculate $E(\mathbb{Q})_{\text{tors}}$ and r.

2.6 Torsion

The torsion subgroup of an elliptic curve is well-understood.

Mazur's Theorem. *For an elliptic curve E over $\mathbb{Q}$ the torsion subgroup $E(\mathbb{Q})_{\text{tors}}$ is one of the following 15 groups*

$$\mathbb{Z}/N\mathbb{Z} \text{ for } 1 \leq N \leq 10 \text{ or } N = 12$$
$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2N\mathbb{Z} \text{ for } 1 \leq N \leq 4$$

This was originally proven by Barry Mazur in [21] and [22]. It is also stated without proof as [29] Theorem VIII.7.5, [18] Chapter 1 Theorem 5.3, and [27] Theorem 2.2.

For our purposes we will only consider the two-torsion of a curve, i.e. the points of order dividing two. Since the group law gives us $-(x, y) = (x, -y)$, it is easy to see that a nonzero point is a two-torsion point if and only if its second coordinate is zero. We will not be overly concerned with the computation of the torsion group of $E(\mathbb{Q})$. It should be noted, however, that the problem of calculating torsion points over the rationals has been solved, and a general algorithm for calculating the torsion group can be found in [9], Section 3.3.

2.7 Torsion in the Congruent Number Curve

On the curve, $E : y^2 = x^3 - n^2x$, we can see that there are four two-torsion points $\{\mathbf{0}, (0, 0), (\pm n, 0)\}$. Since $0, \pm n$ are the only roots of $x^3 - n^2x$, we conclude that these are the only two-torsion points on E. We now show that these are the only torsion points on E following the method in [20].

We begin by calculating the number of points on E over the finite field $\mathbb{F}_p$.

Lemma 2. *Let p be a prime, with $p \nmid n$ and $p \equiv 3 \mod 4$. Then there are exactly $p + 1$ points on E over $\mathbb{F}_p$.*

Proof. The curve E always has the four points $\{\mathbf{0}, (0, 0), (\pm n, 0)\}$. Notice that these remain distinct over $\mathbb{F}_p$ since $p \nmid n$, and p odd. If $p = 3$, then these are the only four points because $0, \pm n$ are the only three possible values of the x-coordinate of a point on E. Let us now examine the points where $x \neq 0, \pm n$. There are $p - 3$ such values for x. We can group them in to pairs $\{\pm x\}$. Now, we have a point on our curve E exactly when $x^3 - n^2x$ is a square in $\mathbb{F}_p$. Since $p \equiv 3 \mod 4$, we know that -1 is not a square in $\mathbb{F}_p$. Since the squares form a subgroup of index 2 in $(\mathbb{F}_p)^*$, we can see that every pair $\{\pm x\}$ in $(\mathbb{F}_p)^*$ contains exactly one square. But we also have that $x^3 - n^2x = -((-x)^3 - n^2(-x))$, so for every pair $\{\pm x\}$, exactly one will lead to a point on our curve in $\mathbb{F}_p$. So we have $(p - 3)/2$ distinct x values. Since each x value leads to exactly two solutions $\pm y$, we have $p - 3$ additional points on E over $\mathbb{F}_p$. Adding in the four two-torsion points, we find there are exactly $p + 1$ points on E over $\mathbb{F}_p$. □

If P_1, P_2 are points on the curve $E(\mathbb{Q})$, we now give a necessary and sufficient condition that $\bar{P}_1 = \bar{P}_2$.

Lemma 3. *Let* $\bar{P}_1, \bar{P}_2 \in \mathbb{P}^2(\mathbb{F}_p)$, *i.e.* $\bar{P}_i = (X_i : Y_i : Z_i)$ *with* $X_i, Y_i, Z_i \in \mathbb{Z}$ *and* $\gcd(X_i, Y_i, Z_i) = 1$. *Then* $\bar{P}_1 = \bar{P}_2$ *iff* p *divides* $Y_1Z_2 - Y_2Z_1, X_2Z_1 - X_1Z_2$ *and* $X_1Y_2 - X_2Y_1$.

Proof. Notice that these are the components of the cross-product of P_1 and P_2 considered as vectors in $\mathbb{R}^3$.
If p divides the cross-product, then we consider two cases.

(1) If p divides X_1, then p divides X_2Z_1 and X_2Y_1. Since p cannot divide both Y_1 and Z_1, we conclude that p divides X_2. Now, we also know $Y_1Z_2 \equiv Y_2Z_1 \mod p$, so we have

$$\begin{aligned}\bar{P}_1 &= (0 : \bar{Y}_1 : \bar{Z}_1)\\ &= (0 : \bar{Y}_1\bar{Y}_2 : \bar{Z}_1\bar{Y}_2)\\ &= (0 : \bar{Y}_1\bar{Y}_2 : \bar{Z}_2\bar{Y}_1)\\ &= (0 : \bar{Y}_2 : \bar{Z}_2)\\ &= \bar{P}_2.\end{aligned}$$

(2) If p does not divide X_1, then

$$\begin{aligned}\bar{P}_2 &= (\bar{X}_2 : \bar{Y}_2 : \bar{Z}_2)\\ &= (\bar{X}_1\bar{X}_2 : \bar{X}_1\bar{Y}_2 : \bar{X}_1\bar{Z}_2)\\ &= (\bar{X}_1\bar{X}_2 : \bar{X}_2\bar{Y}_1 : \bar{X}_2\bar{Z}_1)\\ &= (\bar{X}_1 : \bar{Y}_1 : \bar{Z}_1)\\ &= \bar{P}_1.\end{aligned}$$

For the converse, suppose $\bar{P}_1 = \bar{P}_2$. We know that p does not divide all three of X_1, Y_1, Z_1, so suppose $p \nmid X_1$. The other two cases will proceed in exactly the same

way. Since $\bar{P}_1 = \bar{P}_2$ we have $p \nmid X_2$, thus

$$(\bar{X}_1\bar{X}_2 : \bar{Y}_1\bar{X}_2 : \bar{Z}_1\bar{X}_2) = \bar{P}_1 = \bar{P}_2 = (\bar{X}_1\bar{X}_2 : \bar{X}_1\bar{Y}_2 : \bar{X}_1\bar{Z}_2).$$

Since the first components of these points are the same, we must have $Y_1X_2 \equiv X_1Y_2 \mod p$ and $Z_1X_2 \equiv X_1Z_2 \mod p$. So it only remains to show that $Y_1Z_2 \equiv Y_2Z_1 \mod p$. If p divides both Y_1 and Z_1 this is clear, otherwise replacing X_1, X_2 by Y_1, Y_2 or Z_1, Z_2 in the above argument gives the result. □

Now we are ready to characterize the torsion points of the curve $E : y^2 = x^3 - n^2x$.

Theorem 1. $|E(\mathbb{Q})_{\text{tors}}| = 4$.

Proof. We know there are exactly four two-torsion points on $E(\mathbb{Q})$, $\{\mathbf{0}, (0,0), (\pm n, 0)\}$. Suppose there is another torsion point on $E(\mathbb{Q})$. Since this point is not a two-torsion point it must have order greater than two. Thus the group $E(\mathbb{Q})_{\text{tors}}$ has a subgroup H of order m where either m is odd, or $m = 8$. In fact, Mazur's Theorem (2.6), lists all possible torsion groups, but we do not need such heavy machinery here. Let $H = \{P_1, \ldots, P_m\}$. We now examine for which p the reduction map $P \mapsto \bar{P}$ is injective on H. If we consider $P_1, \ldots, P_m$ as vectors in $\mathbb{R}^3$, since they are distinct in $\mathbb{P}^2(\mathbb{Q})$ no two are multiples of each other, so the cross product $P_i \times P_j \neq \vec{0}$. If we let n_{ij} denote the greatest common divisor of the components of the vector $P_i \times P_j$, by Lemma 3, $\bar{P}_i \neq \bar{P}_j$ if and only if $p \nmid n_{ij}$. So if we let $N = \max(n_{ij})$, we have that the reduction map $P \mapsto \bar{P}$ is injective on H for all primes $p > N$. Thus m divides the order of the group $E(\mathbb{F}_p)$ for all such p. By Lemma 2, if $p \equiv 3 \mod 4$, then $|E(\mathbb{F}_p)| = p + 1$, thus $m \mid p+1$, or $p \equiv -1 \mod m$. Thus we have shown that for all but finitely many primes p with $p \equiv 3 \mod 4$, we have $p \equiv -1 \mod m$. Now recall Dirichlet's famous theorem that for any a, m with $\gcd(a, m) = 1$ there are infinitely many primes p with $p \equiv a \mod m$. (See [19] Chapter 16 Theorem 1). If $m = 8$, we have shown that there are only finitely many primes $p \equiv 3 \mod 8$, which contradicts Dirichlet's Theorem. If m is odd, then for all but finitely many primes $p \equiv 3 \mod 4$ we also have $p \equiv -1 \mod m$ which together give $p \not\equiv 3 \mod 4m$ which is a contradiction to Dirichlet's Theorem if $3 \nmid m$. On the other hand, if $3|m$, then we have if $p \equiv 3 \mod 4$ then for

all but finitely many primes $p \equiv -1 \mod 3k$, so there are only finitely many primes of $p \equiv 7 \mod 12k$ which again contradicts Dirichlet's Theorem. □

Calculating the rank of an elliptic curve is significantly more difficult, and currently no general algorithm is known. The bulk of this thesis will be devoted to finding the rank of certain "congruent number curves".

2.8 Isogenies

An *isogeny*, $\phi : E_1 \to E_2$, is a morphism between elliptic curves E_1 and E_2 such that $\phi(\mathbf{0}_{E_1}) = \mathbf{0}_{E_2}$. In fact ϕ induces a group homomorphism from the group $E_1(K)$ to $E_2(K)$, this is [29] Chapter III Theorem 4.8. We prove a special case of this theorem in §2.9. The map ϕ also induces an injection of function fields by the pull-back,

$$\begin{aligned} \phi^* : K(E_2) &\to K(E_1) \\ f &\mapsto f \circ \phi. \end{aligned}$$

For non-constant ϕ we define the degree of ϕ to be the degree of the field $K(E_1)$ as an extension of the field $\phi^* K(E_2)$. So degree$(\phi) = [K(E_1) : \phi^* K(E_2)]$, where $K(E_1)$ is the rational function field of K over E_1.

If K is a number field, then the Mordell-Weil theorem holds, and we can talk about the *rank* of the curves E_1 and E_2. In this case we have the property that isogenous curves have equal rank. A proof is sketched below.

We have already seen the multiplication-by-m map, denoted $[m]$. It is easy to see that this is in fact an isogeny. This isogeny is particularly important as it exists for all curves E and all positive integers m. For a more thorough discussion of isogenies see [29] Chapter III, Section 4. The degree of the multiplication-by-m map is m^2.

If $\phi : E_1 \to E_2$ is an isogeny of degree m, then there is a unique isogeny of degree m, $\hat{\phi} : E_2 \to E_1$ such that $\hat{\phi} \circ \phi = [m]$. The isogeny $\hat{\phi}$ is called the dual isogeny to ϕ. The existence and uniqueness of the dual isogeny is proven in [29] Theorem III.6.1. Since $\hat{\phi}$ is a homomorphism, $\hat{\phi}$ takes elements of finite order in $E_2(K)$ to elements of finite order in $E_1(K)$. The map $[m]$ takes elements of infinite order to elements of

infinite order and $\hat{\phi} \circ \phi = [m]$, so we must have that ϕ takes elements of infinite order elements of infinite order. This implies that

$$\text{Rank}(E_1(K)) \leq \text{Rank}(E_2(K)).$$

Then, applying the same argument to $\hat{\phi}$, we have that

$$\text{Rank}(E_1(K)) = \text{Rank}(E_2(K)).$$

The fact that isogenous curves have equal rank is useful to us, as we can bound the rank of $E_1(K)$ by bounding the rank of $E_2(K)$.

2.9 2-Isogenies

We now examine in more detail a type of isogeny that will be of use to us. Specifically, we show how to create a degree two-isogeny from any two-torsion point on a curve. We follow the method outlined in [5] Chapter 14.

While it is common, given an elliptic curve, to change variables and write the curve in the form $y^2 = x^3 + ax + b$. In this section, to simplify calculations, we write our elliptic curve in the form $E : y^2 = x(x^2 + ax + b)$. This change of variables has the effect of putting a two-torsion point at $(0, 0)$. Consider a map

$$\begin{aligned} \psi : E &\to E \\ P &\mapsto P + (0,0). \end{aligned}$$

Notice that since $(0, 0)$ is a two-torsion point, we have that $\psi(\psi(x, y)) = (x, y)$. The map $\psi : (x, y) \mapsto (x_1, y_1)$ induces an automorphism on the function field $K(E)$. Let us calculate the fixed field. The line through $(0, 0)$ and (x, y) intersects the curve at a third point, $(x_1, -y_1)$. Solving gives

$$(x_1, y_1) = \left(\frac{b}{x}, \frac{-by}{x^2} \right).$$

Since (x, y) and $(x_1, -y_1)$ are on the same line through the origin, we must have $\frac{y}{x} = \frac{-y_1}{x_1}$, so $\frac{y^2}{x^2}$ is invariant under ψ. Using the fact that $y^2 = x(x^2 + ax + b)$, we have

$$\lambda = \frac{y^2}{x^2} = \frac{x^2 + ax + b}{x}.$$

To find another fixed function, it suffices to notice that $\psi(x, y) = (x_1, y_1)$ and $\psi(x_1, y_1) = (x, y)$ we have that $y + y_1$ is fixed by ψ. Call this value μ. Thus

$$\mu = y - \frac{by}{x^2} = y\left(1 - \frac{b}{x^2}\right).$$

To find a relation between λ and μ notice that

$$\begin{aligned}
\mu^2 &= y^2\left(1 - \frac{b}{x^2}\right)^2 \\
&= \frac{x^2 + ax + b}{x}\left(x^2 - 2x + \frac{b^2}{x}\right) \\
&= \lambda\left(x^2 - 2x + \frac{x^2}{x}\right) \\
&= \lambda\left(\left(x^2 - \frac{b}{x}\right)^2 - 4b\right) \\
&= \lambda\left((\lambda - a)^2 - 4b\right) \\
&= \lambda^2 - 2a\lambda + (a^2 - 4b).
\end{aligned}$$

So we have the equation

$$E_1 : \mu^2 = \lambda^2 - 2a\lambda + (a^2 - 4b). \tag{2.2}$$

We now show that $K(\lambda, \mu)$ is the entire fixed field of ψ. To this end, we solve for x, y in terms of λ, μ. We begin with

$$\sqrt{\lambda} = \frac{y}{x},$$

so

$$\frac{\mu}{\sqrt{\lambda}} = x - \frac{b}{x}.$$

We also have

$$\lambda = \frac{x^2 + ax + b}{x} = x + \frac{b}{x} + a.$$

Combining these gives

$$x = \frac{\lambda + \sqrt{\lambda}\mu - a}{2}, y = \sqrt{\lambda}x.$$

Thus $K(x,y) \subset K(\lambda, \mu, \sqrt{\lambda})$, so $[K(x,y) : K(\lambda,\mu)] \leq 2$. Clearly the field of invariants contains $K(\lambda,\mu)$, so to show that $K(\lambda,\mu)$ is the complete field of invariants, it remains only to show that ψ is not the identity automorphism. This is clear though, since $\psi(x) = \frac{b}{x} \neq x$. Now we are in a position to define the isogeny. Notice that the map ψ has given us another curve E_1 defined be equation (2.2), so we let

$$\phi : E \to E_1$$
$$(x,y) \mapsto (\lambda, \mu)$$

It remains to show that ϕ is, in fact, an isogeny, i.e. ϕ preserves the group law. If P and Q are points on E, then we have seen that there is a function $f \in \mathbb{Q}(x,y)$ with simple poles at P, Q and simple zeros at $\mathbf{0}, P+Q$. To create a function in $\mathbb{Q}(\lambda,\mu)$, we can simply multiply f by its conjugate $\psi(f)$. Thus $f\psi(f)$ is in $\mathbb{Q}(\lambda,\mu)$, and $f\psi(f)$ has simple poles at $\phi(P), \phi(Q)$ and simple zeros at $\mathbf{0}, \phi(P+Q)$ since $\phi(\mathbf{0}) = \mathbf{0}$. Thus $f\psi(f)$ corresponds to the equation

$$\phi(P) + \phi(Q) = \phi(P+Q),$$

which gives us that ϕ is a group homomorphism.

2.10 The Curve $y^2 = x^3 - n^2x$

We are now ready to begin examining the curve E defined by equation (1.2). If n is a congruent number then we have shown how to construct a rational point on the elliptic curve E, from the sides of the triangle with area n. If E has a rational point, this is not enough to guarantee that n is a congruent number, and we will examine the necessary and sufficient conditions below.

To see why every point on E does not correspond to a right triangle with area n, notice, for instance, the points that we can generate from a right triangle all have a square x-coordinate. Points on E that have a non-square x-coordinate were not generated from a right triangle. In fact, a point P on our curve comes from a right triangle if and only if P is twice a rational point, i.e. $P = 2Q$ for some point $Q \in E$. This follows from basic calculations using the addition laws on E. We sketch the correspondence here.

If $Q = (x_0, y_0)$, then the addition law for points (equation 2.1) on E gives

$$2Q = (x_1, y_1) = \left(\frac{1}{4} \frac{(3x_0^2 - n^2)^2}{y_0^2} - 2x_0, y_1 \right).$$

Using the fact that $y_0^2 = x_0^3 - n^2 x_0$, we have

$$\begin{aligned} x_1 &= \left(\frac{x_0^2 + n^2}{2y_0} \right)^2, \\ x_1 - n &= \left(\frac{x_0^2 - 2x_0 n - n^2}{2y_0} \right)^2, \\ x_1 + n &= \left(\frac{x_0^2 + 2x_0 n - n^2}{2y_0} \right)^2. \end{aligned}$$

Thus we find that n is a congruent number (this is just our second definition of a congruent number).

To show the converse, we must find a point (x, y) such that

$$2(x, y) = \left(\left(\frac{c}{2} \right)^2, (a^2 - b^2)\frac{c}{8} \right).$$

Writing out the addition law gives the two equations

$$\frac{1}{4} \frac{(3x^2 - n^2)^2}{y^2} - 2x = \left(\frac{c}{2} \right)^2$$

and

$$\frac{(3x^2 - n^2)\left(3x - \frac{(3x^2 - n^2)^2}{4y^2} \right)}{2y} - y = (a^2 - b^2)\frac{c}{8}.$$

Solving for x and y we find

$$x = \frac{b(b+c)}{2},$$
$$y = \frac{b^2(b+c)}{2}.$$

Thus $2(x,y) = \left(\left(\frac{c}{2}\right)^2, (a^2-b^2)\frac{c}{8}\right)$. Clearly $2((x,y)+P) = 2(x,y)$ for any two-torsion point P. But we know that the two torsion of the curve E is $\{\mathbf{0}, (0,0), (n,0), (-n,0)\}$ (see Theorem (1)), so, in fact, we can find four points which are "half" of the point coming from a right triangle. To effectively use this correspondence, we begin by analyzing which points on E can be twice another point. For our curve E, the situation is rather simple, and since by Theorem 1 we know $E_{\text{tors}}(\mathbb{Q}) = \{\mathbf{0}, (0,0), (\pm n, 0)\}$.

None of these is twice another point because there is no four-torsion. So a square-free natural number n is a congruent number if and only if the curve E defined by (1.2) has positive rank.

For the remainder of the paper we will concern ourselves with finding upper bounds on the rank of E. For an overview of some of the methods and results in the study of ranks of elliptic curves, see [27].

Chapter 3

Two Descent

3.1 Overview

Our goal is to find an upper bound on the rank of the curve E. To that end we will find a bound on the size of the group $E(\mathbb{Q})/2E(\mathbb{Q})$. Since we know $E(\mathbb{Q}) \simeq E(\mathbb{Q})_{\text{tors}} \times \mathbb{Z}^r$, we have

$$|E(\mathbb{Q})/2E(\mathbb{Q})| = |E_{\text{tors}}(\mathbb{Q})/2E_{\text{tors}}(\mathbb{Q})| \cdot |2^r| .$$

For the elliptic curve $E : y^2 = x^3 - n^2x$, we know there are exactly four torsion elements, and $E_{\text{tors}}(\mathbb{Q}) = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, so

$$|E(\mathbb{Q})/2E(\mathbb{Q})| = 4 \cdot |2^r| .$$

In order to bound the size of $E(\mathbb{Q})/2E(\mathbb{Q})$, we construct a homomorphism μ from the group $E(\mathbb{Q})$ with $\ker(\mu) = 2E(\mathbb{Q})$. Thus we have an isomorphism

$$E(\mathbb{Q})/2E(\mathbb{Q}) \simeq \mu(E(\mathbb{Q})).$$

In particular $|E(\mathbb{Q})/2E(\mathbb{Q})| = |\mu(E(\mathbb{Q}))|$. It will be difficult to calculate the group $\mu(E(\mathbb{Q}))$ directly, so we will calculate $\mu(E(\mathbb{Q}_l))$ for various primes l. While $|\mu(E(\mathbb{Q}_l))| \neq |\mu(E(\mathbb{Q}))|$, we can use information about $\mu(E(\mathbb{Q}_l))$ in an attempt to bound the size of $\mu(E(\mathbb{Q}))$.

3.2 The map μ

Consider the elliptic curve $E : y^2 = f(x)$ over a field K, where $f(x) = x^3 + ax + b$. Let $K[\theta] = K[x]/(f(x))$. Set $f = \prod_{i=1}^{n} f_i$ be the factorization of f into irreducibles in $K[x]$. Since f has no repeated roots, f must square-free. In particular the irreducible components f_i are distinct. Then by the Chinese Remainder Theorem, $K[\theta] = \prod_{i=1}^{n} K[x]/(f_i)$.

Let $A_K = K[\theta]$, A_K^* be the group of units in A_K, and let A_K^{*2} be the multiplicative subgroup of A_K^* consisting of the squares of elements in A_K^*.

Define the map μ as follows:

$$\begin{aligned} \mu : E(K) &\to A_K^*/A_K^{*2} \\ (x_0, y_0) &\mapsto (x_0 - \theta) \text{ when } (x_0, y_0) \notin E[2](K). \end{aligned}$$

We know that $(x_0 - \theta) \in A_K^*$ when $(x_0, y_0) \notin E[2](K)$ because then $(x_0 - x)$ is relatively prime to $f(x)$.

When $(x_0, y_0) \in E[2](K)$ we have $f(x_0) = 0$, so $f(x) = (x - x_0)g(x)$ and $K[\theta] \simeq K \times K[x]/(g(x))$. Here we define

$$\begin{aligned} (x_0, 0) &\mapsto (f'(x_0), (x_0 - x) \mod g(x)) \\ \mathbf{0} &\mapsto 1. \end{aligned}$$

We now illustrate the important properties of μ.

Lemma 4. *The map μ is a homomorphism.*

Proof. We follow the proof in [19] Chapter 19. For an alternate proof see [5] Chapter 15 Lemma 1.
We begin by noting that if $P = (x, y)$, then

$$\mu(P) = \mu(x, y) = \mu(x, -y) = \mu(-P)$$

because $\mu(x, y)$ is independent of y. We wish to show that $\mu(P+Q) = \mu(P)\mu(Q)$. Multiplying both sides by $\mu(P)\mu(Q)$, we see that this is equivalent to $\mu(P+Q)\mu(P)\mu(Q) =$

1. Then using the identity above, we see that it is enough to prove $\mu(P+Q)\mu(-P)\mu(-Q) = 1$. Changing notation, we need to show that if $A+B+C = \mathbf{0}$, then $\mu(A)\mu(B)\mu(C) = 1$. Recall that $A + B + C = \mathbf{0}$ is equivalent to stating that A, B, C are collinear. Let $A = (x_1, y_1)$, $B = (x_2, y_2)$ and $C = (x_3, y_3)$. We can also assume that A, B, C are distinct, for if $\mu(P + Q) = \mu(P) + \mu(Q)$ for distinct P, Q, then we have

$$\mu(2P) = \mu(P + Q)\mu(P - Q) = \mu(P)\mu(P)\mu(Q)\mu(Q) = 1 = \mu(P)^2.$$

Now, we divide the proof into cases

- If $x_1 = x_2$ then since $A \neq B$, we must have $B = -A$, which gives $C = \mathbf{0}$, so we have the equation

$$\mu(A)\mu(B)\mu(C) = \mu(A)\mu(-A)\mu(\mathbf{0}) = \mu(A)^2 = 1.$$

- If $x_1 \neq x_2$ and none of the points have order two then, since A, B, C are collinear, there is a line $y = cx + d$ passing through A, B, C. Thus we have

$$f(x) - (cx + d)^2 = (x - x_1)(x - x_2)(x - x_3). \tag{3.1}$$

  Since both sides are monic polynomials of degree three with the same roots. Reducing modulo $f(x)$ and recalling that θ denotes the residue of x, we have

$$(c\theta + d)^2 = (x_1 - \theta)(x_2 - \theta)(x_3 - \theta) \in K[\theta] = K[x]/(f(x)). \tag{3.2}$$

  Noticing the right hand side is just $\mu(A)\mu(B)\mu(C)$ then gives the result.

- If exactly one of the points has order two, then without loss of generality, we may assume $A = (x_1, 0)$. This means that x_1 is a root of f, and writing $f(x) = (x - x_1)g(x)$ as above, we have $K[\theta] = K[x]/(x - x_1) \times K[x]/(g(x))$, and we check each component separately. By the definition of μ we have that

$$\mu(A) = ((x_1 - \theta), (x_0 - x) \mod g(x)),$$

  so the first component of $\mu(A)\mu(B)\mu(C)$ is

$$f'(x_1)(x_2 - x_1)(x_3 - x_1).$$

Since $y = cx + d$ goes through the point $(x_1, 0)$, we have $cx_1 + d = 0$, thus differentiating equation (3.1) and evaluating at $x = x_1$ gives

$$f'(x_1) = (x_2 - x_1)(x_3 - x_1).$$

Thus the first component is just $(f'(x_1))^2$. The fact that the second component is a square follows as in the previous case by reducing equation (3.1) by $g(x)$ and noting that $g|f$.

- If two of the points have order two, then the third point must as well, so that leaves us in the final case that A, B, C all have order two. Thus $y_1 = y_2 = y_3 = 0$. So

$$K[\theta] \simeq K[x]/(x - x_1) \times K[x]/(x - x_2) \times K[x]/(x - x_3).$$

We have

$$\begin{aligned}\mu(A)\mu(B)\mu(C) = &(f'(x_1)(x_2 - x_1)(x_3 - x_1),\\ &(x_1 - x_2)f'(x_2)(x_3 - x_2),\\ &(x_1 - x_3)(x_2 - x_3)f'(x_3))\,.\end{aligned}$$

But differentiating Equation (3.1) and plugging in $x = x_1, x_2$ and x_3 gives

$$\mu(A)\mu(B)\mu(C) = \left((f'(x_1)), (f'(x_2))^2, (f'(x_3))^2\right).$$

□

Lemma 5. $\ker(\mu) = 2E(K)$.

Proof. We follow the proof in [19]. For an alternate proof see [5] Chapter 15 Lemma 2. The kernel of μ clearly contains $2E(K)$ because $\mu(2P) = \mu(P)^2 = 1 \in A_K^*/A_K^{*2}$, so it only remains to show the opposite inclusion. Let $P \in \ker(\mu)$. If $P \neq \mathbf{0}$, we can write $P = (x_0, y_0)$. Since $\mu(P) = 1$, if $2P \neq \mathbf{0}$, it must be that $x_0 - \theta$ is a square in A_K^*. On the other hand, if $2P = \mathbf{0}$, then x_0 is a root of f, so one of the component of $x_0 - \theta$ is zero, and the the others must be squares since $P \in \ker(\mu)$.

Thus we can write

$$x_0 - \theta = (u_0 + u_1\theta + u_2\theta^2)^2 \tag{3.3}$$

for some $u_0, u_1, u_2 \in K$. Since $f(\theta) = 0$, we have $\theta^3 = -a\theta - b$, so we have

$$(u_0 + u_1\theta + u_2\theta^2)(-u_2\theta + u_1) = \underbrace{(-u_0u_2 + u_1^2 + u_2^a)}_{v}\, t + \underbrace{(u_0u_1 + u_2^2b)}_{w}.$$

So $v, w \in K$. Squaring this equation gives

$$(u_0 + u_1\theta + u_2\theta^2)^2(-u_2\theta + u_1)^2 = (v\theta + w)^2.$$

Then substituting equation (3.3) gives

$$(x_0 - \theta)(-u_2\theta + u_1)^2 = (v\theta + w)^2.$$

We must have $u_2 \neq 0$, for otherwise equation (3.3) would not be satisfied. So dividing by u_2^2 we have

$$(x_0 - \theta)(v_2 - \theta)^2 = (v_1\theta + w_1)^2,$$

where $v_2 = u_1/u_2, v_1 = v/u_2, w_1 = w/u_2$. Thus $(v_1x + w_1)^2 - (x_0 - x)(v_2 - x)^2$ is a multiple of $f(x)$. Since they are both monic cubic polynomials, they must be equal, thus

$$f(x) = (v_1x + w_1)^2 - (x_0 - x)(v_2 - x)^2.$$

Now, we can interpret this geometrically. If we consider the line $L : y = v_1x + w_1$, we see that L intersects E at $x = x_0$ and $x = v_2$, with the latter intersection being of multiplicity two. Since three points P, Q, R are collinear iff $P + Q + R = \mathbf{0}$, this gives

$$(x_0, y_0) + 2(v_2, t) = \mathbf{0}$$

for some t. Thus $2(v_2, -t) = (x_0, y_0)$, so $P \in 2E(K)$. □

With these facts in hand we be describe the method of 2-descent.

3.3 The Two-descent

With the above definition of μ we have the exact sequence

$$0 \longrightarrow E[2](K) \longrightarrow E(K) \xrightarrow{2} E(K) \xrightarrow{\mu} A_K^*/A_K^{*2}. \tag{3.4}$$

We will use the fact that μ is an injection from $E(K)/2E(K)$ to A_K^*/A_K^{*2} to bound the rank of E over K. To do this we will make heavy use of the commutative diagram

$$\begin{array}{ccc} E(\mathbb{Q}) & \xrightarrow{\mu} & A_{\mathbb{Q}}^*/A_{\mathbb{Q}}^{*2} \\ \downarrow & & \downarrow{\scriptstyle \psi_l} \\ E(\mathbb{Q}_l) & \longrightarrow & A_{\mathbb{Q}_l}^*/A_{\mathbb{Q}_l}^{*2} \end{array} \tag{3.5}$$

There is no known method for computing the image of μ in A^*/A^{*2}, but it is contained in a finite group which is computable in practice. We define the *2-Selmer Group*, denoted $S^{(2)}(E/\mathbb{Q})$ as

$$S^{(2)}(E/\mathbb{Q}) = \{\delta \in A^*/A^{*2} : \psi_l(\delta) \in \mu(E(\mathbb{Q}_l)) \text{ for all } l\}.$$

The 2-Selmer group contains the image of μ, because if $(x, y) \in E(\mathbb{Q})$, then $(x, y) \in E(\mathbb{Q}_l)$ for all l. Since $\mu(E(\mathbb{Q})) \subset S^{(2)}(E/\mathbb{Q})$, we will attempt to bound $\#\mu(E(\mathbb{Q}))$ by calculating the size of $S^{(2)}(E/\mathbb{Q})$.

In other words, by intersecting the groups $\mu(E(\mathbb{Q}_l))$ with the images $A_{\mathbb{Q}}^*/A_{\mathbb{Q}}^{*2}$ in $A_{\mathbb{Q}_l}^*/A_{\mathbb{Q}_l}^{*2}$ for various l we hope to obtain a bound on the size of $A_{\mathbb{Q}}^*/A_{\mathbb{Q}}^{*2}$, and hence the rank of E over $\mathbb{Q}$.

For a further discussion of the method of 2-Descent see [29] Chapter X, [9] Chapter 3, [3], [19] Chapter 19 or [32].

Chapter 4

Two-descent applied to congruent number curves

Let p be a prime number. We will be working with the elliptic curve:

$$E : y^2 = x(x-p)(x+p).$$

Since $f(x) = x(x-p)(x+p)$ splits completely over $\mathbb{Q}$, we have $A^*_{\mathbb{Q}}/A^{*2}_{\mathbb{Q}} = (\mathbb{Q}^*/\mathbb{Q}^{*2})^3$.

So the map μ becomes

$$\begin{aligned}
\mu : E(\mathbb{Q}) &\rightarrow (\mathbb{Q}^*/\mathbb{Q}^{*2})^3 \\
(x,y) &\mapsto (x, x-p, x+p) \text{ if } x \notin \{0, p, -p, \mathbf{0}\} \\
\mathbf{0} &\mapsto (1,1,1) \\
(0,0) &\mapsto (-1, -p, p) \\
(p,0) &\mapsto (p, 2, p) \\
(-p,0) &\mapsto (-p, -2p, 2).
\end{aligned}$$

Lemma 6. *If $(x,y) \in E(\mathbb{Q})$ then $\mu(x,y) = (\delta_1, \delta_2, \delta_3)$ where each δ_i is in the set $\{1, -1, 2, -2, p, -p, 2p, -2p\}$, and $\delta_1\delta_2\delta_3 \in \mathbb{Q}^{*2}$*

Proof. We have that $\delta_1\delta_2\delta_3 = y^2$. Consider the l-adic valuation of the δ_i's. We have $\mathrm{ord}_l(y^2) = \mathrm{ord}_l(\delta_1\delta_2\delta_3) = \mathrm{ord}_l(\delta_1) + \mathrm{ord}_l(\delta_2) + \mathrm{ord}_l(\delta_3)$ is even for any l. If one of the δ_i's has odd valuation, then two must. If δ_i has odd valuation, then $l \mid \delta_i$, but the δ_i's differ by p or $2p$, so if $l \neq 2, p$, none of the δ_i can have odd valuation. Since we are working modulo squares, we see that if $l \neq 2, p$ the δ_i's must have valuation 0 for all l. So each $\delta_i \in \{1, -1, 2, -2, p, -p, 2p, -2p\}$. □

Lemma 7.

$$\#\mu(E(\mathbb{Q}_l)) = \frac{\#E[2](\mathbb{Q}_l)}{|2|_l}, \tag{4.1}$$

where $|2|_l$ *is the* l*-adic valuation of* 2.

Proof. This is [6] Lemma 5.1 and [7] equation 7.6.2. For an argument using Haar measure see [12] page 451. First notice that since $\ker(\mu(E(\mathbb{Q}_l))) = 2E(\mathbb{Q}_l)$ we have that $\#\mu(E(\mathbb{Q}_l)) = \#E(\mathbb{Q}_l)/2E(\mathbb{Q}_l)$. We will consider two cases, $l < \infty$ and $l = \infty$. If $l < \infty$, then the group $E(\mathbb{Q}_l)$ has a subgroup H of finite index such that $H \simeq \mathbb{Z}_l$. See [29] Theorem VII.6.3. Consider the map

$$\begin{aligned} [2]_H : E(\mathbb{Q}_l)/H &\to 2E(\mathbb{Q}_l)/2H \\ g &\mapsto 2g. \end{aligned}$$

Since H is torsion free, the kernel of map $[2]_H$ is in one-to-one correspondence with the kernel of the map $[2]$, which is $E[2](\mathbb{Q}_l)$, thus

$$|\ker([2]_H)| = |\ker([2])| = \#E[2](\mathbb{Q}_l).$$

This gives us that

$$\#E(\mathbb{Q}_l)/H = (\#2E(\mathbb{Q}_l)/2H) \cdot (\#E[2](\mathbb{Q}_l)).$$

The following equations are true of any abelian groups,

$$\begin{aligned} \#E(\mathbb{Q}_l)/2H &= \#E(\mathbb{Q}_l)/H \cdot \#H/2H \\ \#E(\mathbb{Q}_l)/2H &= \#E(\mathbb{Q}_l)/2E(\mathbb{Q}_l) \cdot \#2E(\mathbb{Q}_l)/2H. \end{aligned}$$

combining these three equations we have

$$\#E(\mathbb{Q}_l)/2E(\mathbb{Q}_l) = \#E[2](\mathbb{Q}_l) \cdot \#\mathbb{Z}_l/2\mathbb{Z}_l.$$

If $l \neq 2$ then $\#\mathbb{Z}_l/2\mathbb{Z}_l = 1$, and if $l = 2$ then $\#\mathbb{Z}_l/2\mathbb{Z}_l = 2$. This proves the lemma for $l < \infty$.

When $l = \infty$, we distinguish two cases depending on how many roots f has in $\mathbb{R}$. If f splits completely over $\mathbb{R}$, we call its roots, $\alpha_1, \alpha_2, \alpha_3$, and we can, without loss of generality, assume $\alpha_1 < \alpha_2 < \alpha_3$. In this case $\#E[2](\mathbb{R}) = 4$ and $\mu : E(\mathbb{R}) \to (\mathbb{R}^*/\mathbb{R}^{*2})^3 \simeq (\mathbb{Z}/2\mathbb{Z})^3$. If (x, y) is a point on the curve, then $\alpha_1 \leq x \leq \alpha_2$ or $\alpha_3 \leq x$, which gives $\mu(x, y) = (x-\alpha_1, x-\alpha_2, x-\alpha_3) = (1, -1, -1)$ or $(1, 1, 1)$. So $\#\mu(E(\mathbb{R})) = 2$. If f has only one root, α_1, over $\mathbb{R}$ then $\#E[2](\mathbb{R}) = 2$ and $\mu(x, y) = (1, 1, 1)$ for all $(x, y) \in E(\mathbb{R})$ since $\alpha_1 \leq x$ for all x, so $\#\mu(E(\mathbb{R})) = 1$.

□

This gives us that $\#\mu(E(\mathbb{Q}_2)) = 8$, $\#\mu(E(\mathbb{R})) = 2$ and $\#\mu(E(\mathbb{Q}_l)) = 4$ for odd l.

4.1 General Bounds

Here we try to find a bound on the size of $\mu(E(\mathbb{Q}))$, and hence the rank of E.

By Lemma 6 we have that

$$\mu(E(\mathbb{Q})) \subset \langle(-1,-1,1), (-1,1,-1), (p,p,1), (p,1,p), (2,2,1), (2,1,2)\rangle.$$

Now $A^*_{\mathbb{R}}/A^{*2}_{\mathbb{R}} = \{(\pm 1, \pm 1, \pm 1)\}$ since $\mathbb{R}^*/\mathbb{R}^{*2} = \mathbb{Z}/2\mathbb{Z}$. We know $\#\mu(E(\mathbb{R})) = 2$ and $\mu((0,0)) = (-1,-1,1)$ so we conclude that $\mu(E(\mathbb{R})) = \{(1,1,1), (-1,-1,1)\}$. Then taking $l = \infty$ in diagram 3.5, we see that $(-1,1,-1) \notin \mu(E(\mathbb{Q}))$.

This shows that $\mu(E(\mathbb{Q}))$ is generated by at most 5 elements, but two of these are the images of two-torsion points, so at most three of these generators can be images of points of infinite order, so we conclude that the rank of $E(\mathbb{Q})$ is at most 3.

4.2 Specific Bounds

In the previous section we found a bound on the size of $\mu(E(\mathbb{Q}))$ that is independent of p. Now we will impose congruence conditions on p to further bound the size of $\mu(E(\mathbb{Q}))$.

For odd p, by (4.1), we have $\#E[2](\mathbb{Q}_p) = \#\mu(E(\mathbb{Q}_p)) = 4$, so we have that

$$\mu(E(\mathbb{Q}_p)) = \{(1,1,1),(-1,-p,p),(p,2,2p),(-p,-2p,2)\}.$$

Note that this is just the image of the 2-torsion points of E. We only wish to keep elements of $\langle(-1,-1,1),(-1,1,-1),(p,p,1),(p,1,p),(2,2,1),(2,1,2)\rangle$ that are equivalent to one of the above elements in $\mathbb{Q}_p$.

We distinguish 4 cases for p

- If $p \equiv 1 \mod 8$, then $-1 \equiv 2 \equiv -2 \equiv 1 \in \mathbb{Q}_p^*/\mathbb{Q}_p^{*2}$ so we eliminate nothing.

$$\mu(E(\mathbb{Q})) \subset \langle(-1,-1,1),(p,p,1),(p,1,p),(2,2,1),(2,1,2)\rangle.$$

- If $p \equiv 3 \mod 8$, then $-2 \equiv 1$ and $-1 \not\equiv 1 \in \mathbb{Q}_p^*/\mathbb{Q}_p^{*2}$ so

$$\mu(E(\mathbb{Q})) \subset \langle(p,p,1),(p,1,p),(-2,-2,1)\rangle.$$

- If $p \equiv 5 \mod 8$, then $-1 \equiv 1$ and $2 \not\equiv -1 \in \mathbb{Q}_p^*/\mathbb{Q}_p^{*2}$ so

$$\mu(E(\mathbb{Q})) \subset \langle(-1,-1,1),(p,p,1),(p,1,p)\rangle.$$

- If $p \equiv 7 \mod 8$, then $2 \equiv 1$ and $-1 \not\equiv 1 \in \mathbb{Q}_p^*/\mathbb{Q}_p^{*2}$

$$\mu(E(\mathbb{Q})) \subset \langle(-1,-p,p),(p,2,2p),(2,2,1),(2,1,2)\rangle.$$

Finally we look at $\mu(E(\mathbb{Q}_2))$. By equation 4.1, $\#\mu(E(\mathbb{Q}_2)) = 8$, so we need 3 generators for the group. The image of the 2-torsion provides 2 generators, the point with $x = 1/4$ happens to map to an independent generator, $(1/4, 1/4 - p, 1/4 + p) \in \mu(E(\mathbb{Q}_2))$.

$$(1/4, 1/4 - p, 1/4 + p) \equiv (1, 1 - 4p, 1 + 4p) \equiv (1, 5, 5) \in \mathbb{Q}_2^*/\mathbb{Q}_2^{*2}.$$

This is because p is odd and so $1 - 4p \equiv 1 + 4p \equiv 5 \mod 8$, so $1 - 4p \equiv 1 + 4p \equiv 5 \in \mathbb{Q}_2^*/\mathbb{Q}_2^{*2}$. This gives us our third generator, so we have that

$$\mu(E(\mathbb{Q}_2)) = \langle(-1, -p, p), (p, 2, 2p), (1, 5, 5)\rangle.$$

Now we remove the elements that are not equivalent modulo squares (in $\mathbb{Q}_2$) to one of the above elements.

We again distinguish 4 cases for p:

- If $p \equiv 1 \mod 8$, then $(-1, -p, p) \equiv (-1, -1, 1)$ and $(p, 2, 2p) \equiv (1, 2, 2) \in \mu(E(\mathbb{Q}_2))$
$$\mu(E(\mathbb{Q})) \subset \langle(-1, -1, 1), (p, p, 1), (p, 1, p), (1, 2, 2)\rangle.$$

- If $p \equiv 3 \mod 8$, then $(-1, -p, p) \equiv (-1, -3, 3)$ and $(p, 2, 2p) \equiv (3, 2, 6) \in \mu(E(\mathbb{Q}_2))$
$$\mu(E(\mathbb{Q})) \subset \langle(-1, -p, p), (p, 2, 2p)\rangle.$$

- If $p \equiv 5 \mod 8$, then $(-1, -p, p) \equiv (-1, -5, 5)$ and $(p, 2, 2p) \equiv (5, 2, 2) \in \mu(E(\mathbb{Q}_2))$
$$\mu(E(\mathbb{Q})) \subset \langle(-1, -1, 1), (-1, p, p), (p, 2, 2p)\rangle.$$
This is because $(-1, -5, 5) \cdot (1, 5, 5) \equiv (-1, -1, 1) \in \mu(E(\mathbb{Q}_2))$.

- If $p \equiv 7 \mod 8$, then $(-1, -p, p) \equiv (-1, 1, -1)$ and $(p, 2, 2p) \equiv (-1, 2, 6) \in \mu(E(\mathbb{Q}_2))$
$$\mu(E(\mathbb{Q})) \subset \langle(-1, -p, p), (p, 2, 2p), (1, 2, 2)\rangle.$$
Because $(-1, 1, -1) \cdot (1, 5, 5) \cdot (-1, 2, 6) \equiv (1, 2, 2) \in \mu(E(\mathbb{Q}_2))$.

4.3 Results

Our results so far can be summarized in the following inequality

$$\text{rank}(E) \leq \begin{cases} 2 \text{ if } p \equiv 1 \mod 8 \\ 0 \text{ if } p \equiv 3 \mod 8 \\ 1 \text{ if } p \equiv 5 \mod 8 \\ 1 \text{ if } p \equiv 7 \mod 8 \end{cases}$$

From here we can already conclude that if $p \equiv 3 \mod 8$, p is not a congruent number. This was already proven in the 19th century by Genocchi in [13] (see [10]). When $p \equiv 5 \mod 8$, or $p \equiv 7 \mod 8$, p is in fact a congruent number. This was stated in [31], and proven in [11] for $p < 10^6$ (p not necessarily prime), and finally proven for all prime p in [24]. Another derivation of the bounds we have obtained on the size of the 2-Selmer group can be found in [17].

If $Ш(E/K)$ were known to be finite, by [29] Chapter X Theorem 4.14, $\#Ш(E/K)[2]$ would have to be a perfect square, thus it would have an even number of generators. The exact sequence

$$0 \longrightarrow E(K)/2E(K) \xrightarrow{\mu} S^{(2)}(E/K) \longrightarrow Ш(E/K)[2] \longrightarrow 0$$

gives us that $\#S^{(2)}(E/K)/\#E(K)/2E(K) = \#Ш(E/K)[2]$. Because $S^{(2)}(E/K)$ has at most 3 generators for $p \equiv 5 \mod 8$, and $p \equiv 7 \mod 8$, this implies that $Ш(E/K)[2]$ must be the trivial group. If $|Ш(E/K)[2]| = 1$ then $E(K)/2E(K) \simeq S^{(2)}(E/K)$, so the rank of $E(\mathbb{Q})$ would have to be exactly 1. For a slightly more in depth discussion of this, see [29] Chapter X, Remark 6.3. While it is not known that $Ш(E/K)[2]$ is finite, it is conjectured to be so, see [29] Chapter X, conjecture 4.13.

We will continue by further analyzing the case when $p \equiv 1 \mod 8$.

Chapter 5

The Case When $p \equiv 1 \mod 8$

5.1 A Specific Two-Isogeny

We have done a 2-descent on the curve $E : y^2 = x(x+p)(x-p)$ in order to bound its rank. To further bound the rank in the case $p \equiv 1 \mod 8$, we will perform a 2-descent on an isogenous curve.

The map

$$\begin{aligned} &\phi : E \to E_1 \\ &(x,y) \mapsto \left(\frac{x^2-p^2}{x}, y + \frac{p^2 y}{x^2}\right) \end{aligned}$$

is an isogeny of degree two generated by the 2-torsion point $(0,0)$, from our curve $E : y^2 = x^3 - p^2 x$ to

$$E_1 = y^2 = x(x^2 + 4p^2).$$

Since $p \equiv 1 \mod 4$, we can write p as the sum of 2 squares in $\mathbb{Z}$. Let $a, b \in \mathbb{Z}$ such that $p = a^2 + b^2$. If we assume $a, b > 0$ and a is odd, then this representation is unique. We will make frequent use of this decomposition of p.

Note that, unlike E, E_1 has only two rational 2-torsion points, $\{\mathbf{0}, (0,0)\}$

5.2 Method

As before, we construct the exact sequence (3.4).

Since $f(x) = x(x^2 + 4p^2)$ does not split completely over $\mathbb{Q}$, we now have two distinct forms for the group A_K^*/A_K^{*2} where μ is defined as follows.

If $i = \sqrt{-1} \in K$, i.e. $f(x)$ splits completely over K, then

$$\begin{aligned} \mu : E_1(K) &\rightarrow (K^*/K^{*2})^3 \\ (x,y) &\mapsto (x, x-2pi, x+2pi) \text{ if } (x,y) \notin E_1[2](K) \\ \mathbf{0} &\mapsto (1,1,1) \\ (0,0) &\mapsto (1,p,p). \end{aligned}$$

When $i \notin K$, we have

$$\begin{aligned} \mu : E_1(K) &\rightarrow K^*/K^{*2} \times K(i)^*/K(i)^{*2} \\ (x,y) &\mapsto (x, x-2pi) \text{ if } (x,y) \notin E_1[2](K) \\ \mathbf{0} &\mapsto (1,1) \\ (0,0) &\mapsto (1,-2pi). \end{aligned}$$

We proceed as before, making use of diagram (3.5), and equation (4.1).

5.3 General Bounds

We begin, as before, by identifying a finite set containing the image of μ.

Lemma 8. $\mu(E_1(\mathbb{Q})) \subset \langle (2, 1+i), (p, a+bi), (p, a-bi), (1,i) \rangle$.

Proof. Suppose $\mu(x,y) = (\delta_1, \delta_2)$. Then we have $\delta_1 \cdot N(\delta_2) = y^2$. Where $N(\delta_1)$ is the norm of δ_2 as an element of the extension field $\mathbb{Q}(i)$, i.e. $N(\delta_2) = \delta_2\bar{\delta_2}$ where $\bar{\delta_2}$ is the ordinary complex conjugate of δ_2. Consider the l-adic valuation of the δ_is. We have $\mathrm{ord}_l(y^2) = \mathrm{ord}_l(\delta_1 \cdot N(\delta_2)) = \mathrm{ord}_l(\delta_1) + \mathrm{ord}_l(N(\delta_2))$ is even for any l. If δ_1 or $N(\delta_2)$ has odd valuation, then they both must. If δ_1 has odd valuation, then $l \mid \delta_1$, but since $\delta_2 = \delta_1 - 2pi$, we have $N(\delta_2) = \delta_1 + 4p^2$. So if $l \mid \delta_1$ and $l \mid \delta_2$ we have that $l \mid 4p^2$, so the only divisors δ_1 are $1, 2, p$. In $\mathbb{Z}[i]$, $4p^2$ factors into irreducibles as $(1+i)^2(1-i)^2(a+bi)(a-bi)$, since every factor of δ_2 is a factor of $4p^2$ the only possible factors of δ_2 are $1, i, 1+i, 1-i, a+bi, a-bi$. The fact that $\mu(E_1(\mathbb{Q})) \subset \langle (2, 1+i), (p, a+bi), (p, a-bi), (1, i) \rangle$ follows from the fact that $\delta_1 \cdot N(\delta_2) \equiv 1$ modulo squares.

□

It is also worthwhile to notice that since we are working modulo squares, $2i \equiv (1+i)^2 \equiv 1$ and so $(2, 1+i)(1, i) \equiv (2, 1-i) \mod$ squares.

5.4 p-adics

Since $E_1[2](\mathbb{Q}_p) = \{\mathbf{0}, (0,0), (2pi, 0), (-2pi, 0)\}$, (4.1) gives that $\#\mu(E_1(\mathbb{Q}_p)) = 4$. The map μ looks like:

$$\begin{aligned}
\mu : E_1(\mathbb{Q}_p) &\to (\mathbb{Q}_p^*/\mathbb{Q}_p^{*2})^3 \\
(x,y) &\mapsto (x, x-2pi, x+2pi) \text{ if } x \notin \{0, 2pi, -2pi, \mathbf{0}\} \\
\mathbf{0} &\mapsto (1,1,1) \\
(0,0) &\mapsto (1,p,p) \\
(2pi,0) &\mapsto (2pi, 2, 4pi) \equiv (p,1,p) \\
(-2pi,0) &\mapsto (-2pi, -4pi, 2) \equiv (p,p,1).
\end{aligned}$$

The last equivalences follow from the fact that 2 and i are squares in $\mathbb{Q}_p$ because

$p \equiv 1 \mod 8$. Since $|\mu(E(\mathbb{Q}_p))| = 4$, we must have that

$$\mu(E_1(\mathbb{Q}_p)) = \{(1,1,1),(1,p,p),(p,1,p),(p,p,1)\}.$$

Now since $(a+bi)(a-bi) = p$, we have that $a+bi \equiv p$ modulo squares and $a-bi \equiv 1$ modulo squares in $\mathbb{Q}_p$ (or vice-versa), and since $(1+i)(1-i) = 2$, which is a square in $\mathbb{Q}_p$, we see that $1+i \equiv i-1$ modulo squares. Before we can eliminate elements from $\mu(E(\mathbb{Q}))$, we must determine when $1+i$ is a square in $\mathbb{Q}_p$.

5.4.1 The Quadratic Character of $1+i$

We have that $p = a^2+b^2$, so $a \equiv bi \mod p$. Using Quadratic Reciprocity and the laws of the Jacobi symbol we have

$$\left(\frac{a}{p}\right) = \left(\frac{p}{a}\right) = \left(\frac{a^2+b^2}{a}\right) = \left(\frac{b^2}{a}\right) = 1.$$

Then $\left(\frac{a+b}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{1+i}{p}\right) = \left(\frac{1+i}{p}\right)$. So we just need to calculate $\left(\frac{a+b}{p}\right)$, which we do using the Jacobi symbol.

$$\left(\frac{a+b}{p}\right) = \left(\frac{p}{a+b}\right) = \left(\frac{2}{a+b}\right)\left(\frac{2p}{a+b}\right) = \left(\frac{2}{a+b}\right)\left(\frac{(a+b)^2+(a-b)^2}{a+b}\right) = \left(\frac{2}{a+b}\right).$$

By Quadratic Reciprocity $\left(\frac{2}{a+b}\right) = (-1)^{\frac{(a+b)^2-1}{8}}$. This gives us that $1+i$ is a quadratic residue mod p exactly when $(a+b)^2 \equiv 1 \mod 16$. We distinguish 2 cases, by the quadratic character of $1+i$.

1. $1+i \equiv \square \in \mathbb{Q}_p$ (i.e. $1+i$ is a square mod p)
   This occurs when $(a+b)^2 \equiv 1 \mod 16$.

$$\begin{array}{lcl} \mu(E(\mathbb{Q})) & \to & \mu(E(\mathbb{Q}_p)) \subset (\mathbb{Q}_p^*/\mathbb{Q}_p^{*2})^3 \\ (2,1+i) & \mapsto & (1,1,1) \\ (2,1-i) & \mapsto & (1,1,1) \\ (p,a+bi) & \mapsto & (p,p,1) \\ (p,1,p) & \mapsto & (p,1,p). \end{array}$$

   In this case, we cannot further reduce the size of $\mu(E(\mathbb{Q}))$.

2. $1+i \not\equiv \square \in \mathbb{Q}_p$ (i.e. $1+i$ is not a square mod p)
   This occurs when $(a+b)^2 \equiv 9 \mod 16$.

$$\begin{aligned}
(2, 1+i) &\mapsto (1, 1+i, 1-i) \notin \mu(E(\mathbb{Q}_p)) \\
(2, 1-i) &\mapsto (1, 1-i, 1+i) \notin \mu(E(\mathbb{Q}_p)) \\
(p, a+bi) &\mapsto (p, p, 1) \\
(p, a-bi) &\mapsto (p, 1, p) \\
(1, i) &\mapsto (1, 1, 1).
\end{aligned}$$

   So $(2, 1+i)$ and $(2, 1-i)$ are not in $\mu(E(\mathbb{Q}))$.

5.5 2-adics

Since $E_1[2](\mathbb{Q}_2) = \{\mathbf{0}, (0,0)\}$, we have, by (4.1), that $\#\mu(E_1(\mathbb{Q}_2)) = 4$ and μ is defined as follows:

$$\begin{aligned}
\mu : E_1(\mathbb{Q}_p) &\to \mathbb{Q}_2^*/\mathbb{Q}_2^{*2} \times \mathbb{Q}_2(i)^*/\mathbb{Q}_2(i)^{*2} \\
(x, y) &\mapsto (x, x - 2pi) \text{ if } x \notin \{0, \mathbf{0}\} \\
\mathbf{0} &\mapsto (1, 1) \\
(0, 0) &\mapsto (1, p).
\end{aligned}$$

Since $\#\mu(E_1(\mathbb{Q}_2)) = 4$ we need to find 2 generators for the group. A little testing yields the points $x = 5$ and $x = 2p$. To see that these are in fact points on the curve $E_1(\mathbb{Q}_2)$, recall that $\mathbb{Q}_2^*/\mathbb{Q}_2^{*2} = \mathbb{Z}/2\mathbb{Z} \times (\mathbb{Z}/8\mathbb{Z})^*$, where an element in $\mathbb{Q}_2$ is a square if and only if it has even valuation (the first term in the product), and the odd part is a square mod 8 (i.e. 1 mod 8). Here we see that $5(5^2 + 4p^2) = 125 + 20p^2 \equiv 5 + 4 \equiv 1$ mod 8, and $2p((2p)^2 + 4p^2) = 8p^3 + 8p^3 = 16p^3$ which is a square because $p \equiv 1$ mod 8.

$$\begin{aligned} \mu(x=5) &= (5, 5-2pi) \equiv (1, 5-2pi) \mod \text{squares} \\ \mu(x=2p) &= (2p, 2p-2pi) \equiv (2, 1+i) \mod \text{squares.} \end{aligned}$$

So we distinguish the same 2 cases as before.

1. $1+i$ is a square in $\mathbb{Q}_p$
   i.e. $(a+b)^2 \equiv 1 \mod 16$

   $$\begin{aligned} \mu(E(\mathbb{Q})) &\to \mu(E(\mathbb{Q}_2)) \subset \mathbb{Q}_2 \times \mathbb{Q}_2(i) \\ (2, 1+i) &\mapsto (2, 1+i) \\ (p, a+bi) &\mapsto (1,1) \\ (p, a-bi) &\mapsto (1,1) \\ (1, i) &\mapsto (1,i) \notin \mu(E(\mathbb{Q}_2)). \end{aligned}$$

   We lose the generator $(2, 1-i)$, which gives us that $\mu(E_1(\mathbb{Q}))$ has at most 3 generators, so we find that in this case the rank of E_1 is at most 2.

2. $1+i$ is not a square in $\mathbb{Q}_p$
   i.e. $(a+b)^2 \equiv 9 \mod 16$

   $$\begin{aligned} (1, p) &\mapsto (1,1) \\ (p, a+bi) &\mapsto (1,5) \notin \mu(E(\mathbb{Q}_2)) \\ (p, a-bi) &\mapsto (1,5) \notin \mu(E(\mathbb{Q}_2)) \\ (1, i) &\mapsto (1,i) \notin \mu(E(\mathbb{Q}_2)). \end{aligned}$$

   So we see that $(p, a+bi)$, $(p, a-bi)$ and $(1, i)$ were not in $\mu(E(\mathbb{Q}))$.

   This gives us that $\mu(E_1(\mathbb{Q})) \subset \langle (1,p) \rangle = \mu(E_1[2](\mathbb{Q}))$ so we conclude that in this case the rank of E_1 is 0.

From this argument we have that if $p \equiv 1 \mod 8$, with a, b such that $a^2 + b^2 = p$ and $(a+b)^2 \equiv 9 \mod 16$, then p is not a congruent number. On the other hand, when $(a+b)^2 \equiv 1 \mod 16$, we cannot make any conclusions. This result was stated

as early as 1915 by L. Bastien [2]. This result can also be obtained as a consequence of Tunnell's Theorem, as in [34] Proposition 6.

Chapter 6

Homogeneous Spaces

6.1 Method

In the previous sections, we have examined the image of the map

$$\begin{aligned} \mu : E(\mathbb{Q}) &\to A^*/A^{*2} \\ P &\mapsto x(P) - \theta, \end{aligned}$$

where, as before $E : y^2 = f(x)$, $A = \mathbb{Q}[x]/(f(x)) = \mathbb{Q}[\theta]$ and θ is the residue of x. As f is a polynomial of degree three, we have that $1, \theta, \theta^2$ is a basis for A, so any element in A can be written as $u_0 + u_1\theta + u_2\theta^2$, where $u_0, u_1, u_2 \in \mathbb{Q}$.

So for any δ in the image of μ we have the equation

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

Expanding the square on the right hand side we have

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

for some quadratic forms $\mathbb{Q}_{\delta,i} \in \mathbb{Q}[u_0, u_1, u_2]$

Equating powers of θ, we have that

$$\begin{aligned} Q_{\delta,2} &= 0 \\ Q_{\delta,1} &= -1. \end{aligned} \tag{6.1}$$

So equations (6.1) gives us a necessary condition for δ to be in the image of μ. These equations are in fact sufficient as well, and if equations (6.1) are satisfied, then $Q_{\delta,0}$ is the x-coordinate of a point on the elliptic curve E.

We would like to restrict our attention to integral solutions to equations (6.1), and this is easily done by noting that $Q_{\delta,1}$ is homogeneous of degree two, and clearing denominators, which gives us the two equations

$$\begin{aligned} Q_{\delta,2} &= 0 \\ Q_{\delta,1} &= -u_3^2. \end{aligned} \tag{6.2}$$

We will begin by examining the equation $Q_{\delta,2} = 0$. If we set

$$C : Q_{\delta,2} = 0.$$

then C is a conic, and if we can find a rational point on C will allow us to parametrize C.

Supposing that we were able to parametrize, C as $(u_0(\lambda), u_1(\lambda), u_2(\lambda))$, we can move on to the second equation, $Q_{\delta,1} = -u_3^2$. Using our parametrization for C, we obtain the equation

$$Q_{\delta,1}(u_0(\lambda), u_1(\lambda), u_2(\lambda)) = -u_3^2.$$

Since $Q_{\delta,1}, Q_{\delta,2}$ are quadratic forms, the left hand side will be a quartic in λ, call it $g(\lambda)$. Then the curve $g(\lambda) = -u_3^2$ has a rational point exactly when δ is in the image of μ.

6.2 Conics

We now examine the homogeneous spaces associated to the curve

$$E_1 : y^2 = x^3 + 4p^2x.$$

We have $f(x) = x^3 + 4p^2x$, which gives $A = \mathbb{Q}[x]/(x^3 + 4p^2x) = \mathbb{Q} \times \mathbb{Q}(i)$.

In the preceding sections we showed that if $p \equiv 1 \mod 8$, then

$$\mu(E(\mathbb{Q})) \subset \langle (2, 1+i), (p, a+bi), (p, a-bi) \rangle.$$

Remember, that when we calculated the δ we used the natural basis $(1,0), (0,1), (0,i)$ of $\mathbb{Q} \times \mathbb{Q}(i)$. We have to convert these into the basis $1, \theta, \theta^2$ where θ is the residue of x in $\mathbb{Q}[x]/(x^3 + 4p^2x) \simeq \mathbb{Q} \times \mathbb{Q}(i)$. To do this, we make explicit the isomorphism

$$\begin{aligned} \mathbb{Q} \times \mathbb{Q}(i) &\simeq \mathbb{Q}(\theta) \\ (1,0) &\leftrightarrow 1 + \frac{1}{4p^2}\theta^2 \\ (0,1) &\leftrightarrow \frac{-1}{4p^2}\theta^2 \\ (0,i) &\leftrightarrow \frac{1}{2p}\theta. \end{aligned}$$

Now we are ready to try to solve the equation $Q_{\delta,2} = 0$ for the allowable values of δ.

- When $\delta = (1,p) = 1 - \frac{p-1}{4p^2}\theta^2$, i.e. δ is the image of the two-torsion point, $(0,0)$. Then we have

$$Q_{\delta,2} = \frac{1}{4}(1-p)u_0^2 - 4p^5u_2^2 + 2p^3u_0u_2 + p^3u_1^2. \tag{6.3}$$

  This has a solution $(0, 2p, 1)$.

- When $\delta = (2, 1+i) = 2 + \frac{1}{2p}\theta + \frac{1}{4p^2}\theta^2$ we have

$$Q_{\delta,2} = 2u_0u_2p^2 + u_1^2p^2 + u_0u_1p - \frac{1}{4}u_0^2 - 4p^4u_2^2 - 4p^3u_1u_2. \tag{6.4}$$

  This has solution $(-2p, 1, 0)$.

- When $\delta = (p, a+bi) = p + \frac{b}{2p}\theta + \frac{(p-a)}{4p^2}\theta^2$ we have

$$Q_{\delta,2} = \frac{1}{4}pu_0^2 + bpu_0u_1 - 4bp^3u_1u_2 - \frac{1}{4}au_0^2 + 2ap^2u_0u_2 + ap^2u_1^2 - 4ap^4u_2^2. \quad (6.5)$$

- When $\delta = (p, a-bi) = p - \frac{b}{2p}\theta + \frac{(p-a)}{4p^2}\theta^2$ we have

$$Q_{\delta,2} = \frac{p-a}{4}u_0^2 - 4bp^3u_0u_1 + 16bp^5u_1u_2 - 4ap^4u_2^2 + 2ap^2u_0u_2 + ap^2u_1^2. \quad (6.6)$$

- When $\delta = (2, 1+i)\cdot(p, a+bi) = 2p + \frac{a+b}{2p}\theta + \frac{2p+b-a}{4p^2}\theta^2$ we have

$$\begin{aligned} Q_{\delta,2} &= (a+b)pu_0u_1 + 2(a-b)p^2u_0u_2 + (a-b)p^2u_1^2 \\ &\quad + \frac{1}{2}pu_0^2 + 4(b-a)p^4u_2^2 - 4(a+b)p^3u_1u_2 + \frac{b-a}{4}u_0^2. \end{aligned} \quad (6.7)$$

- When $\delta = (2, 1+i)\cdot(p, a-bi) = 2p + \frac{a-b}{2p}\theta + \frac{2p-b-a}{4p^2}\theta^2$ have

$$\begin{aligned} Q_{\delta,2} &= (a-b)pu_0u_1 + 2(a+b)p^2u_0u_2 + (a+b)p^2u_1^2 \\ &\quad + \frac{1}{2}pu_0^2 - 4(a+b)p^4u_2^2 - 4(a-b)p^3u_1u_2 - \frac{a+b}{4}u_0^2. \end{aligned} \quad (6.8)$$

- When $\delta = (2, 1+i)\cdot(p, a-bi)\cdot(p, a+bi) = (2, p(1+i)) = 2 + \frac{1}{2}\theta + \frac{2-p}{4p^2}\theta^2$ have

$$Q_{\delta,2} = 2p^2u_0u_2 + p^2u_1^2 + \frac{1}{4}u_0^2 + pu_0u_1 - 4p^4u_2^2 - 4p^3u_1u_2. \quad (6.9)$$

The first equation corresponds to a two-torsion point, so we analyze the only other space with a rational point. From (6.4) for $\delta = (2, 1+i)$, we have

$$C : 2u_0u_2p^2 + u_1^2p^2 + u_0u_1p - \frac{1}{4}u_0^2 - 4p^4u_2^2 - 4p^3u_1u_2 = 0.$$

We know that $(-2p, 1, 0)$ is a point on C, so letting L be the line $u_0 = \lambda u_2 - 2p$, and considering the intersections of L with $Q_{\delta,2}$ as in [25], we arrive at an equation

$$2(\lambda u_2 - 2p)u_2p^2 + p^2 + (\lambda - 2p)p + \frac{1}{4}(\lambda u_2 - 2p)^2 - 4u_2p^4 - 4u_2p^3.$$

Setting this to zero and solving for u_2 we get

$$u_2 = 32\frac{p^3}{\lambda^2 + 8p^2\lambda - 16p^4}.$$

Plugging back in to L we have

$$u_0 = -2p\frac{\lambda^2 - 8p^2\lambda - 16p^4}{\lambda^2 + 8p^2\lambda - 16p^4}.$$

So this gives a parametrization for C as

$$\left(\frac{-2p(\lambda^2 - 8p^2\lambda - 16p^4)}{\lambda^2 + 8p^2\lambda - 16p^4}, 1, \frac{32p^3}{\lambda^2 + 8p^2\lambda - 16p^4}\right).$$

Thus

$$Q_{\delta,1}(u_0(\lambda), u_1(\lambda), u_2(\lambda)) = \frac{-4p(\lambda^4 + 16p^2\lambda^3 - 96p^4\lambda^2 + 768p^6\lambda - 1792p^8)}{(\lambda^2 + 8p^2\lambda - 16p^4)^2}.$$

Absorbing squares into u_3^2, the equation $Q_{\delta,1}(u_0(\lambda), u_1(\lambda), u_2(\lambda)) = -u_3^2$ becomes

$$p(\lambda^4 + 16p^2\lambda^3 - 96p^4\lambda^2 + 768p^6\lambda - 1792p^8) = u_3^2.$$

So if we define

$$f(x) = p(x^4 + 16p^2x^3 - 96p^4x^2 + 768p^6x - 1792p^8),$$

we have that $f(x)$ is an irreducible quartic, and we would like to determine when the equation

$$y^2 = f(x)$$

has solutions We can simplify this by making the change of variable $x \mapsto p^2x$, and $y \mapsto p^4y$, and dividing both sides by p^8, which gives us the equation

$$y^2 = p(x^4 + 16x^3 - 96x^2 + 768x - 1792).$$

Making a further change of coordinates $x \mapsto -4x$ and $y \mapsto 16y$, and dividing both sides by 2^8, we can reduce this to

$$y^2 = p(x^4 - 4x^3 - 6x^2 - 12x - 7). \tag{6.10}$$

Thus we conclude that $(2, 1 + i)$ is in the image of μ exactly when we have a solution to equation (6.10).

6.3 Follow up

The next step would be to find conditions on p such that equation (6.10) has a solution. If we can find a rational solution to equation (6.10), then $(2, 1+i)$ is in the image of μ, which means that the $\#E_1/2E_1 > 2$, so p is a congruent number. On the other hand, if there is no rational solution to equation (6.10), then

$$\mu(E_1(\mathbb{Q})) \subsetneq S^{(2)}(E_1/\mathbb{Q}).$$

We know also that

$$\#S^{(2)}(E_1/\mathbb{Q})/\#\mu(E_1(\mathbb{Q})) = \#Ш[2],$$

so in this case, we must have $\#Ш[2] > 1$.

If, as it is conjectured, $\#Ш < \infty$ then as we argued before, by [29] Chapter X, Theorem 4.14, the order of $Ш[2]$ must be a perfect square, so $\#Ш[2] \geq 4$. Since we have shown in the previous sections that $\#S^{(2)}(E_1/\mathbb{Q}) \leq 8$, we must have $\#\mu(E_1\mathbb{Q}) = 2$, which means that $\text{Rank}(E_1/\mathbb{Q}) = 0$. Thus in this case we conclude that p is not a congruent number.

This gives us a criterion to determine whether p is a congruent number: p is congruent exactly when equation (6.10) has rational solutions.

We have already examined local conditions for the solubility of equation (6.10). In sections 5.4 and 5.5 we examined when $(2, 1+i)$ was in the image of $\mu(E(\mathbb{Q}_p))$ and $\mu(E(\mathbb{Q}_2))$, and we determined that $(2, 1+i)$ was in both images when $(a+b)^2 \equiv 1 \mod 16$. Thus equation (6.10) has solutions $\mathbb{Q}_2$ and $\mathbb{Q}_p$ when $(a+b)^2 \equiv 1 \mod 16$. After testing for local solubility, the standard approach is to perform a second 2-descent on (6.10) as described in [23] and [33] to determine when equation (6.10) has rational solutions. We leave this for a future paper.

Bibliography

[1] Ronald Alter. The congruent number problem. *The American Mathematical Monthly*, 87(1):43–35, 1980.

[2] L. Bastien. Nombres congruents. *Intermédiaire Des Mathématiciens*, 22:231–232, 1915.

[3] B.J. Birch and H.P.F Swinnerton-Dyer. Notes on elliptic curves. I. *Journal für die Reine und Angewandte Mathematik*, 212:7–25, 1963.

[4] B.J. Birch and H.P.F Swinnerton-Dyer. Notes on elliptic curves. II. *Journal für die Reine und Angewandte Mathematik*, 218:79–108, 1965.

[5] J.W.S. Cassels. *Lectures on elliptic curves.* Number 24 in London Mathematical Society Student Texts. Cambridge University Press, 1991.

[6] J.W.S Cassels. Second descents for elliptic curves. *Journal für die Reine und Angewandte Mathematik*, 494:101–127, 1998.

[7] J.W.S. Cassels and E.V. Flynn. *Prolegomena to a Middlebrow Arithmetic of Curves of Genus 2.* Number 230 in London Mathematical Society Lecture Note Series. Cambridge University Press, 1996.

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

[9] John Cremona. *Algorithms for Modular Elliptic Curves.* Cambridge University Press, second edition, 1997.

[10] Leonard Eugene Dickson. *History of the Theory of Numbers Volume*, volume II. American Mathematical Association, 1920.

[11] Noam Elkies. Curves $dy^2 = x^3 - x$ of odd analytic rank. In Claus Fieker and David R. Kohel, editors, *Algorithmic Number Theory, 5th International Symposium, ANTS-V*, pages 244–251, 2002.

[12] E.V. Flynn, B. Poonen, and E. Schaefer. Cycles of quadratic polynomials and rational points on a genus-2 curve. *Duke Mathematical Journal*, 90:435–463, 1997.

[13] Angelo Genocchi. Note analitiche sopra tre scritti. *Annali di Scienze Matematiche e Fisiche*, 6, 1855.

[14] Richard Guy. *Unsolved problems in number theory.* Problem Books in Mathematics. Springer-Verlag, third edition, 2004.

[15] Joe Harris. *Algebraic Geometry: A First Course.* Number 133 in Graduate Texts in Mathematics. Springer-Verlag, 1992.

[16] Robin Hartshorne. *Algebraic Geometry.* Number 52 in Graduate Texts in Mathematics. Springer-Verlag, 1977.

[17] D.R. Heath-Brown. The size of selmer groups for the congruent number problem II. *Inventiones Mathematicae*, 118:331–370, 1994.

[18] Dale Husemöller. *Elliptic Curves.* Number 111 in Graduate Texts in Mathematics. Springer-Verlag, 1987.

[19] Kenneth Ireland and Michael Rosen. *A Classical Introduction To Modern Number Theory.* Number 84 in Graduate Texts in Mathematics. Springer-Verlag, second edition, 1990.

[20] Neal Koblitz. *Introduction to Elliptic Curves and Modular Forms.* Springer-Verlag, second edition, 1993.

[21] Barry Mazur. Modular curves and the eisenstein ideal. *Institut des Hautes Études Scientifiques. Publications Mathématiques*, 47:33–186, 1977.

[22] Barry Mazur. Rational isogenies of prime degree. *Inventiones Mathematicae*, 44(2):129–162, 1978.

[23] J. R. Merriman, S. Siksek, and N. P. Smart. Explicit 4-descents on an elliptic curve. *Acta Arithmetica*, 77(1):385–404, September 1996.

[24] Paul Monsky. Mock heegner points and congruent numbers. *Mathematische Zeitschrift*, 204:45–67, 1990.

[25] Miles Reid. *Undergraduate Algebraic Geometry.* Number 12 in London Mathematical Society Student Texts. Cambridge University Press, 1988.

[26] Joseph J. Rotman. *An Introduction to the Theory of Groups.* Number 148 in Graduate Texts in Mathematics. Springer-Verlag, fourth edition, 1995.

[27] Karl Rubin and Alice Silverberg. Ranks of elliptic curves. *Bulletin of the American Mathematical Society*, 39:455–474, 2002.

[28] Alice Silverberg. Open questions in arithmetic algebraic geometry. *Institute For Advanced Study Park City Mathematics Series*, 9:83–142, 2001.

[29] Joseph H. Silverman. *The Arithmetic of Elliptic Curves.* Number 106 in Graduate Texts in Mathematics. Springer-Verlag, 1986.

[30] William Stein. The group law is a group law. http://modular.fas.harvard.edu/edu/Fall2001/124/lectures/lecture26/lecture26/node3.html.

[31] N.M. Stephens. Congruence properties of congruent numbers. *Bulletin of the London Mathematical Society*, 7:182–184, 1975.

[32] Michael Stoll. Descent on elliptic curves. http://www.faculty.iu-bremen.de/stoll/talks/short-course-descent.pdf.

[33] Michael Stoll. Explicit 4-descent on an elliptic curve. http://modular.math.washington.edu/scans/papers/stoll/4-descent.pdf.

[34] J.B. Tunnell. A classical diophantine problem and modular forms of weight 3/2. *Inventiones Mathematicae*, 72:323–334, 1983.