2015

Elliptic Curves and The Congruent Number Problem

Jonathan Star
Claremont McKenna College

Claremont McKenna College

Elliptic Curves and The Congruent Number Problem

Submitted To

Professor David Krumm

and

Dean Nicholas Warner

by
Jonathan Star

for
Senior Thesis
Spring 2015
April 27, 2015

Contents

Elliptic Curves and The Congruent Number Problem

Jonathan Star

Abstract

In this paper we explain the congruent number problem and its connection to elliptic curves. We begin with a brief history of the problem and some early attempts to understand congruent numbers. We then introduce elliptic curves and many of their basic properties, as well as explain a few key theorems in the study of elliptic curves. Following this, we prove that determining whether or not a number n is congruent is equivalent to determining whether or not the algebraic rank of a corresponding elliptic curve E_n is 0. We then introduce L-functions and explain the Birch and Swinnerton-Dyer (BSD) Conjecture. We then explain the machinery needed to understand an algorithm by Tim Dokchitser for evaluating L-functions at 1. We end by computing whether or not a given number n is congruent by implementing Dokchitser's algorithm with Sage and by using Tunnel's Theorem.

1 The Problem

Definition 1.1 (Congruent Number)**.** A rational number is called **congruent** if it is the area of a rational right triangle—a triangle with three sides of rational length.

For example, $n = 2015$ is a congruent number.

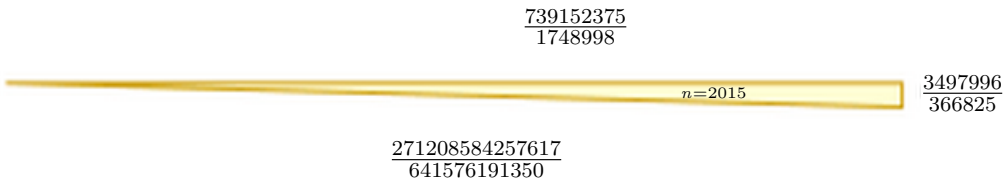

Figure 1.1: A Rational Right Triangle with Area 2015

Clearly every congruent number is rational, but is every positive rational number congruent? We can surmise from Figure 1.1 that generating side lengths of rational right triangles with trial and error is not a realistic approach to figuring out if any given number is congruent. In fact, if we took such an approach we could never be certain that a rational number is not congruent as there are an infinite number of potential values for each side length. The congruent number problem follows naturally:

Problem (The Congruent Number Problem)**.** *Given any rational number r, is there an algorithm to show definitively whether or not r is a congruent number?*

In other words, can we solve the following two equations simultaneously:

$$\begin{cases} a^2 + b^2 = c^2 \\ \frac{ab}{2} = r \end{cases} \tag{1.1}$$

for $a, b, c \in \mathbb{Q}$. If such a, b, and c exist, then r is a congruent number.

Thesis Summary

This paper will discuss progress that mathematicians have made towards solving the congruent number problem, including algorithms currently believed to solve the problem. While this unsolved problem is easy to state, understanding its solution likely requires an understanding of complex machinery and deep mathematical ideas. To this end, this paper aims to provide the reader with an understanding of elliptic curves, one of the most exciting and fertile areas of current research in number theory. Following this brief introduction, Section 2 will provide some history and context of the problem as well as explain its connection to elliptic curves. Section 3 will introduce elliptic curves and provide further background about them. Section 4 will explain the connection between congruent numbers and the algebraic rank of a particular elliptic curve. Section 5 will introduce L-functions and explain the Birch and Swinnerton-Dyer conjecture. Section 6 explains the machinery needed to understand an algorithm to evaluate L-functions at 1. Finally, Section 7 will give two algorithms for determining whether or not a number is congruent—one using machinery from Section 6 and one described by Tunnell's Theorem.

2 Introduction and History

This section will provide some background on the congruent number problem and include some early results. We will provide an alternative statement of the problem, prove that 1 is not a congruent number, and prove that there is a bijection between the set of points (a, b, c) where a, b, c are side lengths of a rational right triangle and (x, y) which are solutions to a particular cubic equation.

We can simplify the congruent number problem by noting that for a given right triangle of area $\frac{ab}{2} = r = \frac{p}{q}$ with $p, q \in \mathbb{Z}$ we can scale the triangle by multiplying each side by q to get a new rational right triangle with area $\frac{abq^2}{2} = rq^2 = pq$. We can deduce that whether or not a rational number r is congruent depends on whether or not a corresponding squarefree integer is congruent. In terms of groups, each coset in $\mathbb{Q}^+/(\mathbb{Q}^+)^2$ has a unique representative that is a squarefree integer. That is, for $r \in \mathbb{Q}^+$ there is a corresponding squarefree integer representative $n \in \mathbb{Q}^+/(\mathbb{Q}^+)^2$. We can therefore safely say that the question of whether r is a congruent number is equivalent to the question of whether n is a congruent number, and from here on we will only talk about congruent numbers as squarefree integers.

The question of whether some number n is a congruent number turns out to be a very hard and very old problem. The history of the congruent number problem is discussed in much detail in Dickson[7]. The first recorded discussion of the problem comes from an anonymous Arabian manuscript written sometime before 972 AD, which states that "the principle object of the theory of rational right triangles is to find a square which when increased or diminished by a certain number (n) becomes a square." The following proposition will demonstrate that this is an equivalent characterization of the congruent number problem.

Proposition 2.1. *A squarefree integer n is a congruent number if and only if there is an integer x such that $x^2 + n$ and $x^2 - n$ is a square.*

Proof. Let n be a congruent number with $a^2 + b^2 = c^2$ and $\frac{1}{2}ab = n$. Multiplying the second equation by 4 and adding or subtracting it to the first, we get

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

Therefore, there exists a rational $x = \frac{c}{2}$ such that $x^2 \pm n$ is a square. If x is an integer such that $x^2 \pm n$ is a square, then $\sqrt{x^2 + n} = u$, $\sqrt{x^2 - n} = v$ are integers. We can form a rational right triangle with sides

$$a = u + v$$
$$b = u - v$$
$$c = \sqrt{a^2 + b^2} = \sqrt{(u+v)^2 + (u-v)^2} = 2x$$

$$\frac{ab}{2} = \frac{(u+v)(u-v)}{2} = \frac{x^2 + n - (x^2 - n)}{2} = n.$$

□

The congruent number problem has vexed many mathematicians over the ages. The term "congruent number" comes from Fibonacci, who, in his work *Liber Quadratorum* (Book of Squares), defined a **congruum** to be an integer n such that $x^2 \pm n$ is a square. The word comes from the Latin word *congruere*, meaning to meet together. Fibonacci proved many facts about congruent numbers. For example, he showed that the product of any square h^2 and 24 is congruent and that multiplying 24 by a sum of squares $1^2+3^2+5^2\cdots$ or the sum $h^2+2h^2+3h^2+\cdots$ yields a congruent number. He stated (without proof) that no square can be a congruent number, claiming that such a case would require integers a and b such that $\frac{a}{b} = \frac{a+b}{a-b}$, an equality which was already known to be impossible. This result is considered to be of great historical importance to the theory of rational right triangles, both because it means that the area of a rational right triangle is not a square and because it implies that the difference of quartics cannot be a square. Fibonacci also proved that if any three of the four numbers $a, b, a+b, a-b$, are squares, then the remaining number is congruent. For example $16, 25$, and 9 are all squares, therefore $16 - 9 = 7$ is a congruent number.

In 1640, Fermat proved that 1 is not a congruent number. The following proof using Fermat's method of descent comes from Conrad [5].

Proposition 2.2 (Fermat)**.** 1 *is not a congruent number.*

Proof. Suppose 1 is a congruent number and let a, b, c, and d be integers with a and b relatively prime (if they aren't we can divide through by $\gcd(a, b)$). We have the following:

$$\left(\frac{a}{d}\right)^2 + \left(\frac{b}{d}\right)^2 = \left(\frac{c}{d}\right)^2, \frac{ab}{2d^2} = 1.$$

This yields a right triangle of area 1 and sides of length $\frac{a}{d}$, $\frac{b}{d}$, and $\frac{c}{d}$. Multiplying through by d^2 we get:

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

which has integer solutions for a, b, c, and d. Because $ab = 2d^2$, either a or b is even and because the two are relatively prime the other is odd, making c odd as well. Without loss of generality we will say a is even and b odd. This combined with $ab = 2d^2$ implies that there are positive integers k and l such that $a = 2k^2$, and $b = l^2$. Substituting for a, we have

$$4k^4 + b^2 = c^2$$

so

$$k^4 = \frac{(c+b)(c-b)}{4} = \frac{(c+b)}{2}\frac{(c-b)}{2}.$$

Now $\gcd(b, c) = 1$ so $\gcd(\frac{c+b}{2}, \frac{c-b}{2}) = 1$, meaning there must be odd integers r, s such that

$$r^4 = \frac{c+b}{2}, s^4 = \frac{c-b}{2}.$$

Solving for b and c,

$$b = r^4 - s^4$$

and

$$c = r^4 + s^4$$

making $l^2 = b = (r^2 + s^2)(r^2 - s^2)$. If $x \in \mathbb{Z}$ is a common factor of $r^2 + s^2$, and $r^2 - s^2$, then are integers n_1, n_2 such that $xn_1 = r^2 + s^2, xn_2 = r^2 - s^2$. It follows that $x(n_1 + n_2) = 2r^2, x(n_1 - n_2) = 2s^2$. Thus any common factor of $r^2 - s^2$ and $r^2 + s^2$ must be odd (l is odd) and divide both $2r^2$ and $2s^2$. However, $\gcd(r, s) = 1$, so $\gcd(r^2 + s^2, r^2 - s^2) = 1$. As $(r^2 + s^2)(r^2 - s^2)$ is an odd square, we can say that $r^2 + s^2 = t^2, r^2 - s^2 = u^2$ for some relatively prime integers t and u. As $r^2 - s^2 = u^2 \equiv 1 \pmod 4$, one of r and s is odd and the other is even. Without loss of generality we say that r is odd and s even. Then

$$r^2 = \frac{t^2 + u^2}{2} = \left(\frac{t+u}{2}\right)^2 + \left(\frac{t-u}{2}\right)^2$$

and we say $a' = (\frac{t+u}{2})^2$, $b' = (\frac{t-u}{2})^2$ and $c' = r$ so

$$(a')^2 + (b')^2 = (c')^2$$

where $\gcd(a', b') = 1$. Note that $0 < c' = r < r^4 < r^4 + s^4 = c$. If we let $d' = s/2$, then we have a new, smaller version of our problem with integer solutions, which is impossible by descent. Therefore 1 cannot be a congruent number. □

The reader may recognize this proof as essentially the same one used to prove Fermat's Last Theorem in the special case for $n = 4$. Fermat famously did not leave a proof of the general case behind (although he claimed to have proved it) and the problem would not be solved until Andrew Wiles's 1995 papers [15, 17]. Wiles's proof required linking Fermat's Last Theorem to seemingly unrelated mathematical objects. Considering that a special case of the congruent number problem is equivalent to a special case of Fermat's Last Theorem, the reader may not be surprised that our approach will do the same. We begin by transforming our congruent number equations in three variables into an equation in two variables.

Proposition 2.3. *Let n be a squarefree positive integer. There is a one-to-one correspondence*

$$\left\{(a, b, c) \in \mathbb{Q}^3 \middle| a^2 + b^2 = c^2, \frac{ab}{2} = n\right\} \longleftrightarrow \left\{(x, y) \in \mathbb{Q}^2 \middle| y^2 = x^3 - n^2 x \text{ and } y \neq 0\right\}$$

with inverse functions

$$(a, b, c) \mapsto \left(\frac{nb}{c-a}, \frac{2n^2}{c-a}\right) \text{ and } (x, y) \mapsto \left(\frac{x^2 - n^2}{y}, \frac{2nx}{y}, \frac{x^2 + n^2}{y}\right).$$

Proof. Let $a, b, c \in \mathbb{Q}$ such that

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

If we let $X = \frac{a}{c}$ and $Y = \frac{b}{c}$, then our new problem is

$$\begin{cases} X^2 + Y^2 = 1 \\ \frac{XY}{2} = \frac{n}{c^2}. \end{cases}$$

The first equation is a circle, which we can parameterize as

$$X = \frac{1 - t^2}{1 + t^2}$$

$$Y = \frac{2t}{1 + t^2}.$$

Letting $w = 1 + t^2$ and plugging into the second equation

$$\frac{(1 - t^2)(2t)}{2w^2} = \frac{n}{c^2}$$

so

$$t - t^3 = n\left(\frac{w}{c}\right)^2.$$

Setting $t = -\frac{x}{n}$ we get

$$-\frac{x}{n} + \frac{x^3}{n^3} = n\left(\frac{w}{c}\right)^2$$

and multiplying through by n^3

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

Set $\frac{n^2 w}{c} = y$ and we have the equation

$$y^2 = x^3 - n^2 x.$$

The opposite direction is easy. First clear y from the denominator and

$$\begin{aligned} (x^2 - n^2)^2 + (2nx)^2 &= x^4 - 2n^2x^2 + n^4 + 4n^2x^2 \\ &= x^4 + 2n^2x^2 + n^4 \\ &= (x^2 + n^2)^2. \end{aligned}$$

Also,

$$\frac{(x^2 - n^2)(2nx)}{2y^2} = \frac{(2)(x^3 - n^2x)(n)}{2y^2} = n$$

□

Remark 2.4. Recall from Proposition 2.1 that if n is a squarefree congruent number, then there is some integer t such that $t^2 \pm n$ is a square. Another way to show the connection between congruent numbers and the equation $y^2 = x^3 - n^2x$ is to consider the arithmetic progression $(t^2 - n, t^2, t^2 + n)$. As all three of these terms are squares, their product is also a square. So there exists a $y \in \mathbb{Z}$ such that

$$y^2 = (t^2 - n)t^2(t^2 + n) = (t^2)^3 - n^2t^2$$

and substituting $x = t^2$ we have

$$y^2 = x^3 - n^2x.$$

Thus if n is congruent then there is a solution to this equation. It is not clear, however, that given a solution to the equation $y^2 = x^3 - n^2x$ one can find a corresponding arithmetic progression. As we will learn in the next section, $y^2 = x^3 - n^2x$ is an example of an elliptic curve.

3 Background on Elliptic Curves

This section introduces elliptic curves and describes some of their properties, including several well known definitions and theorems. For more background on elliptic curves we recommend (in order of accessibility) that the reader see [1], Silverman and Tate [13], Alvaro [12], or [10].

Definition 3.1 (Elliptic Curve)**.** An **elliptic curve** is a non-singular projective curve given by a cubic equation of the form

$$F(X, Y, Z) = aX^3 + bX^2Y + cXY^2 + dY^3 + eX^2Z + fXYZ + gY^2Z + hXZ^2 + jYZ^2 + kZ^3 = 0.$$

Proposition 3.2. *Using an invertible change of variables, any elliptic curve over a field that does not have characteristic* 2 *or* 3 *is given by*

$$zy^2 = x^3 + Axz^2 + Bz^3.$$

Elliptic curves can also be thought of as the set

$$\{(x, y) \big| y^2 = x^3 + Ax + B\} \cup \{\mathcal{O}\}$$

where $\mathcal{O} = (0, 1, 0)$ is the point at infinity. Elliptic curves have an abelian group structure under the operation $\oplus$ with $\mathcal{O}$ as the identity. The operation is defined as follows: Let P and Q be points on an elliptic curve C and let $R' = (X, Y, Z)$ be the third point on $C \cap \overline{PQ}$. Now, let R be the third point on $C \cap \overline{R'\mathcal{O}}$. Then $P \oplus Q = R$, as shown in Figure 3.1. Note that if $R' = (X, Y, 1)$, then $R = (X, -Y, 1)$.

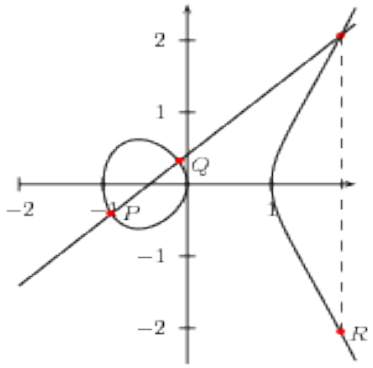

Figure 3.1: Elliptic Curve Addition for $P \neq Q$

If $P = Q$, let ℓ be the tangent line through P and let R' be the third point at which C and ℓ intersect. Once again if R is the third point on $C \cap \overline{R'\mathcal{O}}$ then $P \oplus Q = R$ as shown in Figure 3.2. If $P = Q$ and ℓ is vertical then $P + Q = \mathcal{O}$.

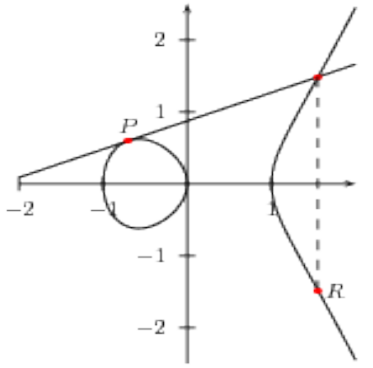

Figure 3.2: Elliptic Curve Addition for $P = Q$

Theorem 3.3 (Mordell-Weil Theorem)**.** *Let E be an elliptic curve over the rationals. Then the group of rational points on E, $E(\mathbb{Q})$, is finitely generated.*

Definition 3.4 (Algebraic Rank of an Elliptic Curve)**.** From group theory, $E(\mathbb{Q}) \cong E(\mathbb{Q})_{\text{tors}} \oplus \mathbb{Z}^r$ for some nonnegative integer r. We call r the **algebraic rank** of E.

Said differently, r is the number of points of infinite order required (in conjunction with the torsion points) to generate E. Finding the rank of an elliptic curve can be a difficult problem, particularly for curves of larger ranks (at present the elliptic curve with the highest known rank has $r \geq 28$ [9]). In this paper we will be concerned with the rank of elliptic curves that correspond to congruent numbers.

Definition 3.5 (E_n)**.** E_n is the elliptic curve given by the equation

$$y^2 = x^3 - n^2 x.$$

Definition 3.6 (Discriminant)**.** Let C be a cubic of the form

$$x^3 + Ax + B$$

then the **discriminant** of C is

$$\Delta C = -16(4A^3 + 27B^2).$$

In particular,

$$\Delta E_n = 64n^6.$$

Definition 3.7 (Reduction Modulo p Map)**.** The reduction modulo p map is a map $\phi : \mathbb{P}^2_{\mathbb{Q}} \to \mathbb{P}^2_{\mathbb{F}_p}$ that maps a point $(x, y, z) \to (\tilde{x}, \tilde{y}, \tilde{z})$, where $\tilde{x} \equiv x \pmod{p}$.

Definition 3.8 (Reduction Curve)**.** $E_n(\mathbb{F}_p)$ (often denoted $\tilde{E}_n$) is the reduction curve modulo p of $E_n(\mathbb{Q})$.

Definition 3.9 (Primes Of Good Reduction)**.** Given a non-singular cubic curve C, we call p a **prime of good reduction** if the reduction modulo p map is injective. Equivalently, p is a prime of good reduction if p does not divide $2\Delta C$. If p is such a prime, we say that C has good reduction modulo p. If p is not such a prime, we say that p is a **prime of bad reduction** and that C has bad reduction modulo p.

Theorem 3.10 (Mazur's Theorem)**.** *Let C be an elliptic curve and suppose that $C(\mathbb{Q})$ contains a point of finite order m. Then either*

$$1 \leq m \leq 10 \text{ or } m = 12.$$

Specifically, the torsion points of $C(\mathbb{Q})$ form a finite subgroup that is either

1. *a cyclic group of order N for $1 \leq N \leq 10$ or $N = 12$.*
2. *the product of a cyclic group of order 2 and another cyclic group of order $2N$ with $1 \leq N \leq 4$.*

Theorem 3.11 (Nagell-Lutz Theorem)**.** *Let E be an elliptic curve over the rationals with discriminant D and let $P = (x, y)$ be a rational point on E of finite order. Then x and y are integers and either*

$$\begin{cases} (1)\ y = 0 \text{ (in which case } 2P = \mathcal{O}) \\ (2)\ y | D. \end{cases}$$

Theorem 3.11 makes finding the torsion points on an elliptic curve over the rationals considerably easier. Note that 3.11 implies that the rational points (x, y)on E_n that do not correspond to solutions to equation 1.1—points with $y = 0$ (Proposition 2.3)—have order 2. Finding the torsion points on E_n will prove crucial to understanding the connection between elliptic curves and congruent numbers. Specifically we will use this information to draw conclusions about the connection between the rank of E_n and whether or not n is congruent.

4 Congruent Numbers and Algebraic Rank

In this section we will show that a squarefree integer n is congruent if and only if the curve E_n has positive rank. To prove this we will construct an injective map from $E_n(\mathbb{Q})_{\text{tors}}$ to $E_n(\mathbb{F}_p)$ and use this information to show that E_n has exactly four torsion points—none of which correspond to a rational right triangle as detailed in Proposition 2.3.

Lemma 4.1. *Let $P = (x_1, y_1, z_1)$ and $Q = (x_2, y_2, z_2)$. Then P and Q map to the same point in $\mathbb{P}^2_{\mathbb{F}_p}$ if and only if $p|x_1y_2 - x_2y_1$, $p|x_2z_1 - x_1z_2$, and $p|y_1z_2 - y_2z_1$.*

Proof. Suppose that $\tilde{P} = (\tilde{x}_1, \tilde{y}_1, \tilde{z}_1) = (\tilde{x}_2, \tilde{y}_2, \tilde{z}_2) = \tilde{Q}$. Because $\gcd(x_1, y_1, z_1) = 1$, p does not divide all three. WLOG, if $p \nmid x_1$, we can deduce that p does not divide $\tilde{x}_1, \tilde{x}_2$. So

$$\begin{aligned}(\tilde{x}_1\tilde{x}_2, \tilde{x}_1\tilde{y}_2, \tilde{x}_1\tilde{z}_2) &= (\tilde{x}_2, \tilde{y}_2, \tilde{z}_2)\\ &= \tilde{Q}\\ &= \tilde{P}\\ &= (\tilde{x}_1, \tilde{y}_1, \tilde{z}_1)\\ &= (\tilde{x}_2\tilde{x}_1, \tilde{x}_2\tilde{y}_1, \tilde{x}_2\tilde{z}_1)\end{aligned}$$

Because $\tilde{x}_1\tilde{x}_2 = \tilde{x}_2\tilde{x}_1$, it must be the case that $\tilde{x}_1\tilde{y}_2 = \tilde{x}_2\tilde{y}_1$ and $\tilde{x}_1\tilde{z}_2 = \tilde{x}_2\tilde{z}_1$. So it stands to reason that $p|x_1y_2 - x_2y_1$, and $p|x_1z_2 - x_2z_1$. Note that $p|y_1 \Leftrightarrow p|y_2$, in which case $p|y_1z_2 - z_2y_1$. If $p \nmid y_1$ we can repeat the above process to get the same result. Now suppose $p|x_1y_2 - x_2y_1$, $p|x_2z_1 - x_1z_2$, and $p|y_1z_2 - y_2z_1$. If $x_1|p$, then WLOG $p \nmid y_1$. Because $p|x_1y_2 - x_2y_1$ and $x_1y_2 \equiv 0 \pmod p$, it must be that $x_2y_1 \equiv 0 \pmod p$. But $p \nmid y_1$, so $p|x_2$, which implies that $\tilde{x_1} = \tilde{x_2} = 0$. So $\tilde{P} = (0, \tilde{y}_1, \tilde{z}_1)$ and $\tilde{Q} = (0, \tilde{y}_2, \tilde{z}_2)$. Therefore,

$$\begin{aligned}\tilde{P} &= (0, \tilde{y}_1, \tilde{z}_1)\\ &= (0, \tilde{y}_1\tilde{y}_2, \tilde{z}_1\tilde{y}_2)\\ &= (0, \tilde{y}_1\tilde{y}_2, \tilde{z}_2\tilde{y}_1)\\ &= (0, \tilde{y}_1, \tilde{z}_1)\\ &= \tilde{Q}\end{aligned}$$

as $\tilde{z}_1\tilde{y}_2 = \tilde{z}_2\tilde{y}_1$. Now if $p \nmid x_1, y_1$, and z_1, then

$$\begin{aligned}\tilde{P} &= (\tilde{x}_1, \tilde{y}_1, \tilde{z}_1) \\ &= (\tilde{x}_1\tilde{x}_2, \tilde{x}_2\tilde{y}_1, \tilde{x}_2\tilde{z}_1) \\ &= (\tilde{x}_1\tilde{x}_2, \tilde{x}_1\tilde{y}_2, \tilde{x}_1\tilde{z}_2) \\ &= (\tilde{x}_2, \tilde{y}_2, \tilde{z}_2) \\ &= \tilde{Q}.\end{aligned}$$

This concludes the proof of the lemma. □

Theorem 4.2. *Let $\phi : E_n(\mathbb{Q})_{\text{tors}} \to E_n(\mathbb{F}_p)$ be the reduction modulo p map. Then $E_n(\mathbb{Q})_{\text{tors}}$ injects into $E_n(\mathbb{F}_p)$ for all but finitely many p.*

Proof. By the above lemma, if $P \in E_n(\mathbb{Q})_{\text{tors}}$ has coordinates (x_i, y_i, z_i) for $0 < i \leq \#E_n(\mathbb{Q})_{\text{tors}}$, then two points $\tilde{P}_i = \tilde{P}_j$ when $p|x_1y_2 - x_2y_1$, $p|x_2z_1 - x_1z_2$, and $p|y_1z_2 - y_2z_1$. That is to say that $E_n(\mathbb{Q})_{\text{tors}}$ injects into $E_n(\mathbb{F}_p)$ when

$$(\tilde{x}_i\tilde{y}_j - \tilde{x}_j\tilde{y}_i, \tilde{x}_i\tilde{z}_j - \tilde{x}_j\tilde{z}_i, \tilde{y}_i\tilde{z}_j - \tilde{y}_j\tilde{z}_i) \neq (0, 0, 0).$$

So if $d_{i,j} = \gcd(x_iy_j - x_jy_i, x_iz_j - x_jz_i, y_iz_j - y_jz_i)$ and $D = \text{lcm}(d_{i,j})$ for all $0 < i, j \leq \#E_n(\mathbb{Q})_{\text{tors}}$, then $\phi : E_n(\mathbb{Q})_{\text{tors}} \to E_n(\mathbb{F}_p)$ is an injection so long as $p \nmid D$.

□

Proposition 4.3. *Let*

$$E_n : y^3 = x^3 + n^2x.$$

If $p \in \mathbb{Z}$ is a prime congruent to $3 \pmod 4$, then $\#E_n(\mathbb{F}_p) = p + 1$.

Proof. We can immediately see that there are four points of order 1 or 2: $\mathcal{O}, (0, 0), (n, 0)$, and $(-n, 0)$. $\#E_n(\mathbb{F}_p)$ is finite, so we are simply going to count the real points on E_n that are not $(0, 0), (\pm n, 0)$. Note that $f(x) = y^2 = x^3 - n^2x$ is an odd function and that -1 is not a square in $\mathbb{F}_p$ because $p \equiv 3 \pmod 4$ (-1 is not a quadratic residue $\pmod p$). We start by arranging all possible x values of E in pairs $\{x, -x\}$. There are at most $p - 3$ points, or $\frac{p-3}{2}$ pairs $\{x, -x\}$. It is easy to see that $f(x)$ and $f(-x) = -f(x)$ cannot both be squares as if $f(x)$ is a square then $-1f(x)$ is a nonsquare. Similarly, if $f(-x)$ is a square, then $-f(-x) = f(x)$ is a nonsquare. If we choose whichever of $\pm x$ makes f a square, we get exactly two points for each representative: $\{x, \pm\sqrt{f(x)}\}$ or $\{-x, \pm\sqrt{f(-x)}\}$. There are $\frac{p-3}{2}$ pairs of points times 2 points per pair plus four points of order 1 or 2, leaving $p+1$ points in $\mathbb{F}_p$ that lie on $E_n(\mathbb{F}_p)$.

□

Theorem 4.4 (Dirichlet's Theorem on Primes in Arithmetic Progressions)**.** *Given $a, d \in \mathbb{Z}$ with $\gcd(a, d) = 1$, there are infinitely many primes congruent to $a \pmod d$.*

Lemma 4.5. *Let $m > 4$ be an integer. Then there exist infinitely many primes $p \equiv 3 \pmod 4$ such that $m \nmid p+1$.*

Proof. Suppose m is a power of 2. Then $m = 2^a$ for some $a \geq 3$. By Dirichlet's Theorem on Arithmetic Progressions there are an infinite number of primes $p \equiv 3 \pmod m$. But if $m|p-3$ and $4|m$, then $4|p-3$ so $p \equiv 3 \pmod 4$. $p+1 \equiv 4 \pmod m$ and so cannot be congruent to $0 \pmod m$. Therefore, $m \nmid p+1$ for an infinite number of primes p.

If m is not a power of 2, then it must have some odd prime divisor $q|m$. By the Chinese Remainder Theorem, there exists an integer x such that

$$\begin{cases} x \equiv 1 \pmod q \\ x \equiv 3 \pmod 4. \end{cases}$$

This means that $q \nmid x$, and as q is an odd prime $\gcd(q, x) = 1$. We also know that x is not even as $x \equiv 3 \pmod 4$, so $\gcd(4q, x) = 1$. By Theorem 4.4 , there are an infinite number of primes p such that $p \equiv x \pmod 4q$. So $4qk = p - x$ for $k \in \mathbb{Z}$. Thus $q|p-x$ and $4|p-x$, meaning

$$\begin{cases} p \equiv x \equiv 3 \pmod 4 \\ p \equiv x \equiv 1 \pmod q. \end{cases}$$

So for an infinite number of primes p, $p \not\equiv -1 \pmod q$. Then $q \nmid p+1$, which implies $m \nmid p+1$, leaving us with an infinite number of primes congruent to $3 \pmod 4$ such that $m \nmid p+1$. □

Proposition 4.6. *Let n be a squarefree positive integer. Then*

$$E_n(\mathbb{Q})_{\text{tors}} = \{\mathcal{O}, (0,0), (n,0), (-n,0)\}.$$

Proof. It is trivial to see that $\mathcal{O}, (0,0), (n,0), (-n,0) \in E_n(\mathbb{Q})_{\text{tors}}$ so we need only to show that $m = \#E_n(\mathbb{Q})_{\text{tors}} \leq 4$. Theorem 4.2 allows us to construct an injective homomorphism $\phi : E_n(\mathbb{Q})_{\text{tors}} \mapsto E_n(\mathbb{F}_p)$. This implies that $E_n(\mathbb{Q})_{\text{tors}}$ is isomorphic to a subgroup of $E_n(\mathbb{F}_p)$ and hence

$$m|\#E_n(\mathbb{F}_p)$$

for all primes of good reduction. By Proposition 4, $m|p+1$ for all but finitely many primes (those of bad reduction) congruent to $3 \pmod 4$. If $m > 4$, then from Lemma 4.5 there are an infinite number of primes congruent to $3 \pmod 4$ such that $m \nmid p+1$. This is a contradiction and therefore $m \leq 4$. Thus $\#E_n(\mathbb{Q})_{\text{tors}} = 4$ and specifically

$$E_n(\mathbb{Q})_{\text{tors}} = \{\mathcal{O}, (0,0), (n,0), (-n,0)\}.$$

□

Remark 4.7. Lemma 4.5 and Proposition 4.6 are not the standard proofs that $E_n(\mathbb{Q})_{\text{tors}} = \{\mathcal{O}, (0,0), (n,0), (-n,0)\}$. The standard proof can be found in Koblitz [10]

Theorem 4.8. *Let n be a squarefree positive integer. Then n is a congruent number if and only if the rank of E_n is positive.*

Proof. In the forward direction, let n be a congruent number and let a, b, c be the lengths of a right triangle with area n. By Proposition 2.3 there is a rational point (x, y) such that $y \neq 0$ on $E_n(\mathbb{Q})$. Proposition 4.6 implies that (x, y) is not a torsion point on $E_n(\mathbb{Q})$. Thus E_n has non-zero rank. In the other direction, if the rank of E_n is non-zero then there exists a point P of infinite order on $E_n(\mathbb{Q})$. This means that there is a rational solution to $y^2 = x^3 - n^2x$ with $y \neq 0$ and by Proposition 2.3 n is a congruent number.

□

We have now proved that the congruent number problem reduces to the problem of whether E_n has positive rank. How do we find out whether E_n has positive rank? This is a decidedly easier problem than actually computing the rank of an elliptic curve but it is still sufficiently difficult that we need to develop more machinery. In particular, we will need to learn some of the properties of L-functions and how they can provide information about elliptic curves.

5 L-Functions and Elliptic Curves

In this section we introduce L-functions and provide intuition for why we evaluate them at $s = 1$. We then explain the Birch and Swinnerton-Dyer Conjecture and show that, if true, then a number n is congruent if and only if $L(E_n, 1) = 0$.

Definition 5.1 (L-Function)**.** An **L-function** is an infinite series of the form

$$L(s) = \sum_{n=1}^{\infty} a_n n^{-s}$$

where $a_n \in \mathbb{C}$.

Definition 5.2 (N_p and a_p)**.** For E_n we define $N_p = \#E_n(\mathbb{F}_p)$. When $E_n(\mathbb{F}_p)$ is non-singular (p is of good reduction) we define

$$a_p = p + 1 - N_p.$$

When $E_n(\mathbb{F}_p)$ is singular we define

$$a_p = p - N_p.$$

Theorem 5.3 (Hasse's Theorem)**.** $|a_p| \leq 2\sqrt{p}$

Definition 5.4 (L-Function of an Elliptic Curve)**.** Let S be the set of primes of bad reduction for an elliptic curve E and s a complex number. The L-function associated with E is defined as

$$L(E,s) = \prod_{p \in S} \frac{1}{1 - a_p p^{-s}} \prod_{p \notin S} \frac{1}{1 - a_p p^{-s} + p^{1-2s}}$$

where p is prime and $s \in \mathbb{C}$.

Remark 5.5. We have defined an L-function as an infinite sum, yet we have also defined $L(E,s)$ as an infinite product. If this seems contradictory, note that by the formula for an infinite geometric series

$$\frac{1}{1 - a_p p^{-s}} = 1 + a_p p^{-s} + (a_p p^{-s})^2 + (a_p p^{-s})^3 + \cdots$$

and

$$\frac{1}{1 - (a_p p^{-s} - p^{1-2s})} = 1 + (a_p p^{-s} - p^{1-2s}) + (a_p p^{-s} - p^{1-2s})^2 + (a_p p^{-s} - p^{1-2s})^3 + \cdots$$

so our infinite product is equal to an infinite sum which satisfies the definition of an L-function.

If we wish to use the L-function to understand more information about elliptic curves it is natural to ask the question of where the L-function for a particular elliptic curve is convergent and where it is divergent. Let $s = \sigma + it$ be a complex number. Then

$$\sum_{n=0}^{\infty} |a_n n^{-s}| = \sum_{n=0}^{\infty} |a_n||n^{-s}| = \sum_{n=0}^{\infty} |a_n||n^{-\sigma - it}| = \sum_{n=0}^{\infty} |a_n||e^{-\sigma \log(n)}||e^{-it \log(n)}|.$$

However, n is a positive real number so $|e^{-it \log(n)}| = 1$. Whether or not an L-function converges therefore depends only on the real part of s. A simple comparison test shows that if $\sigma_1 < \sigma_2$ and an L-function converges at $\Re(s) = \sigma_1$ then it also converges at $\Re(s) = \sigma_2$. Thus, L-functions converge in a half plane $\Re(s) \geq \sigma$ for some sigma.

Theorem 5.6. *Let $s = \sigma + i\tau$ be a complex number. If $\sum_{n=1}^{\infty} n^{1/2-\sigma}$ converges, then $L(E,s)$ converges.*

This theorem is a consequence of Theorem 5.3 (Hasse's Theorem). The idea is to use the bound $|a_p| \leq 2\sqrt{p}$ to derive a bound for each individual a_n. If p, q are primes such that $n = pq$, we can see from Definition 5.4 and Remark 5.5 that the only terms in $L(E,s)$ of the form $c_0 p^{-s}$ and $c_1 q^{-s}$ (where c_0, c_1 are complex constants) are $a_p p^{-s}$ and $a_q q^{-s}$ respectively. Thus $a_n = a_p a_q$ and $|a_n| = |a_p||a_q| \leq (2\sqrt{p})(2\sqrt{q}) = 4\sqrt{n}$. So if n has k prime factors then $a_n \leq 2^k \sqrt{n}$. Thus $\sum_n^{\infty} a_n n^{-s}$ converges if $\sum_n^{\infty} 2^k n^{1/2} n^{-s}$ converges,

where k is the number of prime factors of n. It is easy to see that Theorem 5.6 holds if we allow n to be only prime numbers. Although we will not prove it here, Theorem 5.6 does hold when we allow n to be composite as well.

Corollary 5.7. *$L(E, s)$ converges in $\Re(s) > 3/2$.*

Proof. We know from calculus that $\sum_{n=1}^{\infty} n^{-x}$ converges when $x > 1$. Therefore, $L(E, s)$ converges when $1/2 - \sigma \leq -1$, or when $\Re(s) > \frac{3}{2}$.

□

Theorem 5.8. *$L(E, s)$ has an analytic continuation to the entire complex plane*[1].

In particular, we will be interested in $L(E, 1)$. To give some intuition for why we evaluate the function at one, consider the following partial product:

$$\prod_{p \in S} \frac{1}{1 - a_p p^{-s}} \prod_{p \notin S, p \leq x} \frac{1}{1 - a_p p^{-s} + p^{1-2s}}$$

where $x \in \mathbb{Z}$. In essence we are truncating the L-function at $p \leq x$ in order to make it easier to handle. If we let $s = 1$, then

$$\begin{aligned} L(E,1) \text{ truncated at } p \leq x &= \prod_{p \in S} \frac{1}{1 - a_p p^{-1}} \prod_{p \notin S, p \leq x} \frac{1}{1 - a_p p^{-1} + p^{-1}}. \\ &= \prod_{p \in S} \frac{1}{1 - a_p p^{-1}} \left(\frac{p}{p}\right) \prod_{p \notin S, p \leq x} \frac{1}{1 - a_p p^{-1} + p^{-1}} \left(\frac{p}{p}\right) \\ &= \prod_{p \in S} \frac{p}{p - a_p} \prod_{p \notin S, p \leq x} \frac{p}{p - a_p + 1} \\ &= \prod_{p \leq x} \frac{p}{N_p}. \end{aligned}$$

Therefore, one way to think about $L(E, 1)$ is to think about

$$\lim_{x \to \infty} \prod_{p \leq x} \frac{p}{N_p}.$$

Evaluating the L-function of an elliptic curve at 1 therefore has a connection to the relationship between p and N_p. It is this insight which prompted Birch and Swinnerton-Dyer's famous conjecture:

[1]This is a consequence of a very big theorem called the modularity theorem due to results by Wiles [17], Taylor and Wiles [15], Diamond [6], Conrad, Diamond and Taylor [4], and Breuil, Conrad, Diamond, and Taylor [3]. We restate and give a brief explanation of the theorem in the next section.

Conjecture 5.9 (BSD Conjecture (weak form))**.** *If r is the algebraic rank of an elliptic curve E, then $L(E,1)$ has a zero of order r. Equivalently, the Taylor expansion of $L(E,s)$ around $s=1$ has the form*

$$c_0(s-1)^r + c_1(s-1)^{r+1} + c_2(s-1)^{r+2} + ...$$

where all c_i are complex constants and $c_0 \neq 0$.

A stronger form of BSD specifies the value of c_0, but we will not include it here. As BSD is only a conjecture it is useful to have another name for the actual order of vanishing of $L(E,1)$.

Definition 5.10 (analytic rank)**.** If $L(E,s)$ has a Taylor expansion around 1

$$L(E,1) = c_0(s-1)^\rho + c_1(s-1)^{\rho+1} + c_2(s-1)^{\rho+2} + ...$$

with $c_0 \neq 0$, then we call ρ the **analytic rank** of E.

Thus the BSD conjecture says that the analytic rank of an elliptic curve is equal to its algebraic rank. For clarity, we will always specify when talking about analytic rank, whereas if we use the term "rank" alone we refer to the algebraic rank of a curve.

Theorem 5.11. *If BSD holds, then $L(E_n,1)=0$ if and only if n is a congruent number.*

Proof. If n is not a congruent number then by Theorem 4.8 the rank of $E_n = 0$. By BSD the analytic rank $\rho = 0$ so $L(E,1)$ has a constant term c_0. All other terms $c_i(s-1)^{\rho+i} = 0$ so $L(E_n,1) \neq 0$. Thus if $L(E_n,1) = 0$, then n is a congruent number. Similarly, if $L(E_n,1) \neq 0$ then it must have a constant term. This implies that the analytic rank of E_n is 0 which implies by BSD and Theorem 4.8 that n is not a congruent number. Thus if n is a congruent number, then $L(E_n,1) = 0$. □

This is intuitively sound. Recall that $L(E_n,1)$ can be thought of as $\lim_{x\to\infty} \prod_{p\leq x} \frac{p}{N_p}$. From Theorem 5.3 we can deduce that as p grows larger and larger $\frac{p}{N_p}$ tends to 1. Thus it is not clear at first glance whether $L(E_n,1) = 0, 1$, or ∞. However, the more points on $E_n(\mathbb{Q})$, the more points that might be on the reduction curve $E(n)(\mathbb{F}_p)$. It is therefore reasonable to expect N_p to be larger on average for curves with an infinite number of points that might reduce $\pmod p$ than for curves with a finite number of points that might reduce $\pmod p$. Thus N_p is more likely to be larger than p when E_n has positive rank (n is congruent), making the infinite product $\prod_{p\leq x} \frac{p}{N_p}$ tend to 0 as x tends to infinity.

Theorem 5.12 (Kolyvagin)**.** *Weak BSD holds if E has analytic rank of 0 or 1.*

Theorem 5.12 can be quite useful as most elliptic curves (at minimum over 66%) are of rank 0 or 1 [2]. Thus, we now need only to compute analytic rank in order to discover the rank of most elliptic curves. In the next section we will state definitions and theorems necessary to understand an algorithm for computing $L(E,1)$.

6 Evaluating $L(E, 1)$

In this section we describe the machinery needed to understand an algorithm by Tim Dokchitser [8] to evaluate the L-function of an elliptic curve at $s = 1$. In doing so we will touch on modular forms and the modularity theorem, along with other topics.

Dokchitser's algorithm for computing L-functions reduces to the following equation in the case of when evaluating at $s = 1$:

Theorem 6.1 (Dokchitser)**.**

$$L(E, 1) = (2)(1 + w_E) \sum_{n=1}^{\infty} a_n n^{-1} \int_{(n\pi(\sqrt{N})^{-1})}^{\infty} \phi(x) dx.$$

What follows is a collection of definitions and theorems needed to understand this statement.

Definition 6.2 (Node and Cusp)**.** Let $P = (x_0, y_0) \in E(\mathbb{F}_p)$ be a singular point, and let

$$y - y_0 = \alpha(x - x_0) \text{ and } y - y_0 = \beta(x - x_0)$$

be the equations of the tangent lines to $E(\mathbb{F}_p)$ at P. If $\alpha \neq \beta$ for some α, β then we call P a **node**. Otherwise we call P a **cusp**.

Definition 6.3 (Additive and Multiplicative Reduction)**.** For a prime p of bad reduction, if $E(F_p)$ has a cusp it is said to have **additive reduction** and if it has a node it is said to have **multiplicative reduction**.

Definition 6.4 (Conductor of E)**.** The **conductor**, N_E, of E_n is defined as

$$N_E = \prod_{p \notin S} p^{f(p)}$$

where

$$f(p) = \begin{cases} 0 & p \text{ is of good reduction} \\ 1 & p \text{ has multiplicative reduction} \\ \geq 2 & p \text{ has additive reduction} \end{cases}$$

We will not detail values of $f(p)$ for primes of additive reduction but the important thing is that N_E encodes information about the type of reduction that E has at each prime.

Definition 6.5 (Gamma Function)**.** The **gamma function** is defined as

$$\Gamma(z) = \int_0^{\infty} e^{-t} t^{z-1} dt$$

where $z \in \mathbb{C}$.

Definition 6.6 (Mellin Transform)**.** The **Mellin transform** of a function $f(x)$ is the integral

$$\mathcal{M}f(x) = \phi(x) = \int_0^\infty x^{t-1} f(x) dx$$

with inverse

$$\mathcal{M}^{-1}\phi(x) = f(x) = \frac{1}{2\pi i} \int_{c-i\infty}^{c+i\infty} x^{-s} \phi(s) ds$$

where the inverse is only valid given certain conditions.

Definition 6.7 (Modular Form)**.** Let $\mathbb{H} = \{a + bi : a, b \in \mathbb{R}, b > 0\}$ be the upper half of the complex plane. A **modular form** is a function $f : \mathbb{H} \to \mathbb{C}$ that satisfies certain relations, including periodicity relations. If f has a power series expansion

$$f(z) = \sum_{n>0} b_n e^{2\pi i n z}$$

then it is called a **cuspidal modular form** (or a **cusp form** for short).

Definition 6.8 (Modular Form for $SL_2(\mathbb{Z})$)**.** Define the group

$$SL_2(\mathbb{Z}) = \{\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid a, b, c, d \in \mathbb{Z}, \det \gamma = 1\}$$

where γ acts on a complex number z as $\gamma z = \frac{az+b}{cz+d}$. Modular Forms for the group $SL(2, \mathbb{Z})$ satisfy the following properties:

1. f is analytic on $\mathbb{H}$
2. $f(\gamma z) = (cz + d)^k f(z)$
3. f has a power series expansion $f(z) = \sum_{n \geq 0} b_n e^{2\pi i n z}$

where k is called the **weight** of f. We say that f is **modular** if conditions 1 and 2 are satisfied and f has a power series expansion $f(z) = \sum_{n \geq N_0} b_n e^{2\pi i n z}$ where $N_0 < 0$ is an integer.

Note that $\gamma_1 = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ and $\gamma_2 = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ are both elements of $SL_2(\mathbb{Z})$. Thus, modular forms of weight k for $SL_2(\mathbb{Z})$ have the relations $f(\gamma_1 z) = f(\frac{-1}{z}) = z^k f(z)$ and $f(\gamma_2 z) = f(z + 1) = f(z)$.

Theorem 6.9 (The Modularity Theorem)**.** *For every elliptic curve E, there exists a cusp form f_E of weight 2 such that $L(E, s) = L(f_E, s)$ where*

$$L(f_E, s) := \sum_{n=0}^{\infty} b_n n^{-s} = \prod_{p \text{ prime}} \frac{1}{1 - b_p p^{-s} + p^{k-1-2s}}.$$

Put differently, for every prime p, $a_p = b_p$. Note that at weight $k = 2$, the term $k-1-2s$ used in $L(f_E, s)$ is equal to $1 - 2s$, which is the term used in $L(E, s)$ (Definition 5.4).

As we mentioned in the footnote to Theorem 5.8, this is an extremely important theorem due to results by Wiles [17], Taylor and Wiles [15], Diamond [6], Conrad, Diamond and Taylor [4], and Breuil, Conrad, Diamond, and Taylor [3]. Without the modularity theorem it does not even make sense to talk about $L(E, 1)$ as it is not clear that $L(E, 1)$ converges. For this reason the modularity theorem is essential to this paper's approach to the congruent number problem. That Birch and Swinnerton-Dyer formulated their conjecture in the early 1960s—roughly 40 years before the first piece of the modularity theorem was proved—is nothing short of remarkable.

Definition 6.10. Let E be an elliptic curve and s a complex number. Then

$$\Lambda(E, s) := \frac{(\sqrt{N_E})^s}{(2\pi)^s}\Gamma(s)L(E, s).$$

Theorem 6.11. *$\Lambda(E, s)$ is analytic in the entire complex plane and satisfies the functional equation*

$$\Lambda(E, 2 - s) = w_E\Lambda(E, s)$$

where $w_E = \pm 1$.

Remark 6.12. We call w_E the **root number**. It is a product of all local root numbers w_p, which equal 1 if p is a prime of good reduction and -1 for some primes of bad reduction. The root number for E_n is known to be -1 when $n \equiv 5, 6, 7 \pmod 8$ and 1 when $n \equiv 1, 2, 3 \pmod 8$ [10].

At $s = 1$, $2 - s = s$. This provides a natural motivation for examining $\Lambda(E, s)$ (and so also $L(E, s)$) at $s = 1$. Λ is analytic so it has a Taylor series expansion around $s = 1$

$$\Lambda(E, s) = c(s - 1)^\rho + \text{ h.o.t.}$$

where $c \neq 0$ and h.o.t. are the higher order terms of the Taylor expansion. The same applies for $\Lambda(E, 2 - s)$:

$$\Lambda(E, 2 - s) = c_1((2 - s) - 1)^\rho + \text{ h.o.t} = c_1(1 - s)^\rho + \text{ h.o.t} = uc_1(s - 1)^\rho + \text{ h.o.t}$$

where $u = 1$ if ρ is even and -1 if ρ is odd. If we go back to our functional equation we have

$$uc_1(s - 1)^\rho + \text{ h.o.t} = \Lambda(E, 2 - s) = w_E\Lambda(E, s) = wc_1(s - 1)^\rho + \text{ h.o.t}$$

so $w_E = u$. ρ of course is the analytic rank of E, so BSD leads naturally to the following conjecture:

Conjecture 6.13 (Parity Conjecture)**.** *Let ρ be the analytic rank of E and r the algebraic rank. Then*

$$w_E = (-1)^\rho = (-1)^r.$$

If the Parity Conjecture holds then $w_E = -1$ when the rank of E is odd, which means that E must have positive rank. Specifically this implies that if $w_{E_n} = -1$, then n is a congruent number. Recall from Remark 6.12 that w_{E_n} is known to be -1 when $n \equiv 5, 6, 7 \pmod 8$. So if the Parity Conjecture is true, then all $n \equiv 5, 6, 7 \pmod 8$ are congruent numbers.

We now can turn our attention to calculating $L(E, 1)$. Most algorithms for doing so, including Dokchitser's, involve a series of functions derived from Mellin transforms of the analytic continuation of $L(E, s)$. The following is Tim Dokchitser's algorithm, simplified to apply to $L(f_E, 1)$, which is equal to $L(E, 1)$ by the Modularity Theorem.

Theorem 6.14 (Dokchitser)**.**

$$\Lambda(f_E, 1) = (1 + w_E) \sum_{n=1}^{\infty} a_n \frac{\sqrt{N_E}}{n\pi} \int_{(n\pi(\sqrt{N_E})^{-1})}^{\infty} \phi(x)dx$$

where ϕ is the inverse Mellin transform of the gamma function.

Theorem 6.1 follows from the definition of Λ:

$$L(E, 1) = (2)(1 + w_E) \sum_{n=1}^{\infty} a_n n^{-1} \int_{(n\pi(\sqrt{N_E})^{-1})}^{\infty} \phi(x)dx.$$

We now have a working understanding of Dokchitser's algorithm. In the next section we now will use the algorithm to determine whether certain numbers are congruent.

7 Is n a Congruent Number?

In this section we will test whether or not several numbers are congruent using Dokchitser's algorithm and Tunnell's Theorem.

We have now shown that there is a bijection between the set of solutions to our congruent number equations (equation 1.1) and the number of rational points on the elliptic curve E_n (Proposition 2.3). We have further shown that a squarefree integer n is congruent if and only if E_n has positive rank (Theorem 4.8). We have also shown that if the widely believed Birch and Swinnerton-Dyer conjecture is true, then E_n has positive rank if and only if the $L(E_n, 1) = 0$ (Theorem 5.11). In the previous section we described an algorithm that we can use to compute $L(E_n, 1)$, and thus—if BSD holds or the analytic rank of E_n is less than two (Theorem 5.12)—solve the congruent number problem. We will now use that algorithm to determine whether various squarefree integers n are congruent numbers. To do this we will be using Sage [14], which has built in functionality for Dokchitser's Algorithms.

Example 7.1. We use Dokchitser's algorithms in Sage to find the L-function associated with E_n for $n = 210$, a known congruent number (the area of a right triangle of lengths 20, 21, and 29). We define the curve E_{210} and its associated L-function in Sage as follows:

```
E210=EllipticCurve([-44100,0])        # 210^{2}=44100
L210=E210.lseries().dokchitser().

L210.taylor_series(1,4)
```

computes the Taylor series for us which gives us the expansion around $s = 1$ of

$$L(E_{210}, 1) \approx -1.25903\times10^{-23}+5.43688\times10^{-23}(s-1)+16.86665(s-1)^2-72.83542(s-1)^3+\cdots+$$

which one can see has an analytic rank of 2 (as the first two terms of the approximation are so close to zero). We can evaluate the L-function at 1 and the algebraic rank of E_{210} with the code

```
L210(1)
```

and

```
E6.rank().
```

We find that $L(E_{210}, 1) = 0$, and E_{210} has rank 2. By Theorem 4.8 and Corollary 5.11, we confirm that 210 is indeed a congruent number.

Example 7.2. We use Sage to approximate the expansion for $L(E_2, 1)$.

```
E2=EllipticCurve([-4,0])
L2=E2.lseries().dokchitser()
L2.taylor_series(1,4)
```

yields the approximation

$$L(E_2, 1) \approx 0.92703 + 0.31116(s - 1) - 0.38477(s - 1)^2 + 0.23061(s - 1)^3 + \cdots$$

Clearly the analytic rank is 0, and indeed

```
L2(1)
L2.rank()
```

gives a value of .92703 a rank of 0, meaning that (if BSD holds) 2 is not a congruent number.

Example 7.3. We use Sage to determine whether or not 2015 is a congruent number.

```
E2015=EllipticCurve([-4060225,0])
E2015.rank()
```

calculates the rank of E_{2015} to be 1, so 2015 is a congruent number. Accordingly,

```
L2015=E2015.lseries().dokchitser()
L2015.taylor_series(1,4)
```

computes that

$$L(E_{2015}, 1) \approx 0 + 15.53490(s-1) - 107.59707(s-1)^2 + 481.03503(s-1)^3 + \cdots .$$

Now that we know that 2015 is a congruent number, suppose we wish to construct a rational right triangle of area 2015. Sage has functionality to identify points on an elliptic curve.

```
E2015.an_element()
```

yields the projective coordinate $(\frac{83265625}{40401} : \frac{159596067500}{8120601} : 1)$. Using Proposition 2.3 we can find rational side lengths a, b, and c of such a triangle:

$$a = \frac{(\frac{83265625}{40401})^2 - 2015^2}{\frac{159596067500}{8120601}}$$

$$b = \frac{(2)(2015)(\frac{83265625}{40401})}{\frac{159596067500}{8120601}}$$

$$c = \frac{(\frac{83265625}{40401})^2 + 2015^2}{\frac{159596067500}{8120601}}.$$

Doing the calculations,

$$a = \frac{3497996}{366825}, b = \frac{739152375}{1748998}, \text{ and } c = \frac{271208584257617}{641576191350}.$$

This is the method that we used to generate Figure 1.1.

Computing the L-function at $s = 1$ is not the only way to determine if n is congruent. In 1983, Tunnell used modular forms of weight $\frac{3}{2}$ to prove a simple algorithm for finding n, which was conditioned on the BSD holding true [16].

Theorem 7.4 (Tunnell's Theorem)**.** *Let n be a squarefree positive integer. Define*

$$n_1 = \#\{x, y, z : n = x^2 + 2y^2 + 8z^2\}$$

$$n_2 = \#\{x, y, z : n = x^2 + 2y^2 + 32z^2\}$$

$$n_3 = \#\{x, y, z : n = 2x^2 + 8y^2 + 16z^2\}$$

$$n_4 = \#\{x, y, z : n = 2x^2 + 8y^2 + 64z^2\}.$$

If n is odd and a congruent number, then $n_1 = 2n_2$. If n is even and congruent then $n_3 = 2n_4$. Conversely, if the weak Birch-Swinnerton Dyer Conjecture holds for E_n, then if n is odd and $n_1 = 2n_2$ or if n is even and $n_3 = 2n_4$, then n is a congruent number.

Tunnell's Theorem gives us a relatively simple, computationally finite algorithm for testing whether or not a number is congruent. We give a few examples below using the code provided in appendix A to calculate n_1, n_2, n_3, and n_4 and implement Tunnell's Theorem.

Example 7.5. We show that Tunnell's Theorem holds by checking a known congruent number. Let $n = 210$ (the area of a right triangle of lengths $20, 21$, and 29). In this case $n_1 = n_2 = n_3 = 16$ and $n_4 = 8$, so $n_3 = 2n_4$.

Example 7.6. We check whether or not 2 is a congruent number. Let $n = 2$. $n_1 = \#\{x, y, z : 2 = x^2 + 2y^2 + 8z^2\} = 2$, as the only solutions occur when $y = \pm 1$. Similarly $n_2 = x^2 + 2y^2 + 32z^2 = 2$. $n_1 \neq 2n_2$. 2 is odd and not a square so by Tunnell's theorem 2 is not a congruent number. This agrees with Example 7.2.

Example 7.7. We check whether or not 2015 is a congruent number. Here $n_1 = n_2 = n_3 = n_4 = 0$, so 2015 is a congruent number.

Example 7.8. We use Tunnell's Theorem to check a larger number: $n = 373522$. Then $n_1 = 456, n_2 = 456, n_3 = 456, n_4 = 232$. n is even and so by Tunnell's theorem is congruent if $n_3 = 2n_4$. $(2)(232) = 464 \neq 456$. Thus 373522 is not a congruent number.

Example 7.9. We show that any squarefree positive integer n congruent to $5, 6$, or $7 \pmod 8$ is a congruent number. Let $n \equiv 5$ or $7 \pmod 8$. Note that $8z^2 \equiv 32z^2 \equiv 0 \pmod 8$. Only $0, 1$, and 4 are squares $\pmod 8$, so $x^2 + 2y^2 \not\equiv n \pmod 8$. Therefore, $n \neq x^2 + 2y^2 + 8z^2$ making $n_1 = 0$ and similarly $n_2 = 0$. Since $n_1 = 2n_2$, by Tunnell's Theorem n is a congruent number. Now let $n \equiv 6 \pmod 8$. Then $n - 6 = 8k$ for some $k \in \mathbb{Z}$ so $n - 3 = 4(k)$ and $\frac{n}{2} \equiv 3 \pmod 4$. But only 0 and 1 are squares $\pmod 4$ which means that $x^2 \not\equiv \frac{n}{2} \pmod 4$ making $n_3 = 0 = 2n_4$. By Tunnell's Theorem n is again not a congruent number.

8 Conclusion

This paper has presented two algorithms for solving the congruent number problem. The first, due to Dokchitser, is very difficult to compute but comparatively easy to explain. The second, due to Tunnel, is easy to compute but has a more difficult proof. In a sense this is fitting as the congruent number problem is at once simple and complex. We began with a very simple problem—among the oldest unsolved problems in mathematics. In each section we translated the problem into another, less recognizable problem until we eventually arrived at Dokchitser's algorithm that utilizes complicated machinery, some of which we have only loosely defined. While our approach may not give the reader a precise understanding of what Dokchitser's algorithm is, it provides a the reader a clear understanding of why it works.

Acknowledgements

I would like to thank Professor David Krumm for introducing me to the congruent number problem, for his help throughout this process, and for his infinite patience.

9 Appendix A

The following Java code uses Tunnell's Theorem to evaluate whether or not a squarefree integer, n, is a congruent number.

```
import java.lang.Math;
import java.util.*;

public class tunnell {

 /**
  * this class asks the user to input a squarefree integer and
     ↪ prints whether
  * or not it is a congruent number
  *
  */

 public tunnell() {
 }

 /**
  * returns n1
  *
  * @param int n
  *
  */
 public int solven1(int n) {
  int order = 0;
  for (int x = (int) -Math.sqrt((double) n); x <= (int) Math
    .sqrt((double) n); x++) {
   for (int y = (int) -Math.sqrt((double) n); y <= (int) Math
     .sqrt((double) n); y++) {
    for (int z = (int) -Math.sqrt((double) n); z <= (int) Math
      .sqrt((double) n); z++) {
     if (x * x + 2 * y * y + 8 * z * z == n) {
      order++;
     }
    }
   }
  }
  return order;
```

```
}

/**
 * returns n2
 *
 * @param int n
 *
 */

public int solven2(int n) {
 int order = 0;
 for (int x = (int) -Math.sqrt((double) n); x <= (int) Math
   .sqrt((double) n); x++) {
  for (int y = (int) -Math.sqrt((double) n); y <= (int) Math
    .sqrt((double) n); y++) {
   for (int z = (int) -Math.sqrt((double) n); z <= (int) Math
     .sqrt((double) n); z++) {
    if (x * x + 2 * y * y + 32 * z * z == n) {
     order++;
    }
   }
  }
 }
 return order;
}

/**
 * returns n3
 *
 * @param int n
 *
 */

public int solven3(int n) {
 int order = 0;
 for (int x = (int) -Math.sqrt((double) n); x <= (int) Math
   .sqrt((double) n); x++) {
  for (int y = (int) -Math.sqrt((double) n); y <= (int) Math
    .sqrt((double) n); y++) {
   for (int z = (int) -Math.sqrt((double) n); z <= (int) Math
     .sqrt((double) n); z++) {
```

```
    if (2 * x * x + 8 * y * y + 16 * z * z == n) {
     order++;
    }
   }
  }
 }
 return order;
}

/**
 * returns n4
 *
 * @param int n
 *
 */

public int solven4(int n) {
 int order = 0;
 for (int x = (int) -Math.sqrt((double) n); x <= (int) Math
   .sqrt((double) n); x++) {
  for (int y = (int) -Math.sqrt((double) n); y <= (int) Math
    .sqrt((double) n); y++) {
   for (int z = (int) -Math.sqrt((double) n); z <= (int) Math
     .sqrt((double) n); z++) {
    if (2 * x * x + 8 * y * y + 64 * z * z == n) {
     order++;
    }
   }
  }
 }
 return order;
}

/**
 * returns true if n is odd and false if it is even
 *
 * @param int n
 *
 */

public boolean isOdd(int n) {
```

```
 if (n % 2 != 0)
  return true;
 return false;
}

/**
 * Implements Tunnells theorem calling and returns true if n is
    ↪ a congruent
 * number
 *
 * @param int n
 *
 */

public static boolean isCongruent(int n) {

 tunnell t = new tunnell();

 int n1 = t.solven1(n);
 int n2 = t.solven2(n);
 int n3 = t.solven3(n);
 int n4 = t.solven4(n);

 System.out.println("n1 = " + n1);
 System.out.println("n2 = " + n2);
 System.out.println("n3 = " + n3);
 System.out.println("n4 = " + n4);

 if (t.isOdd(n)) {
  if (n1 == 2 * n2)
   return true;
  return false;
 }

 if (n3 == 2 * n4)
  return true;
 return false;
}

/**
 * asks the user to input a squarefree integer and prints
```

```
    ↪ whether or not it
  * is congruent
  *
  * @param args
  */
 public static void main(String[] args) {

  System.out.println("Please enter a squarefree integer");

  Scanner scan = new Scanner(System.in);
  int n = scan.nextInt();

  if (isCongruent(n))
   System.out.println("n is a congruent number");
  else {
   System.out.println("n is not a congruent number");
  }
 }

}
```

References

[1] Avner Ash and Robert Gross, *Elliptic tales*, Princeton University Press, Princeton, NJ, 2012. Curves, counting, and number theory.

[2] Manjul Bhargava, Christopher Skinner, and Wei Zhang, *A majority of elliptic curves over* $\mathbf{Q}$ *satisfy the birch and swinnerton-dyer conjecture* (July 17, 2014), available at `1407.1826`.

[3] Christophe Breuil, Brian Conrad, Fred Diamond, and Richard Taylor, *On the modularity of elliptic curves over* $\mathbf{Q}$*: wild 3-adic exercises*, J. Amer. Math. Soc. **14** (2001).

[4] Brian Conrad, Fred Diamond, and Richard Taylor, *Modularity of certain potentially Barsotti-Tate Galois representations*, J. Amer. Math. Soc. **12** (1999).

[5] Keith Conrad, *The congruent number problem.* `http://www.math.uconn.edu/~kconrad/blurbs/ugradnumthy/congnumber.pdf`.

[6] Fred Diamond, *On deformation rings and Hecke rings*, Ann. of Math. (2) **144** (1996).

[7] Leonard Eugene Dickson, *History of the theory of numbers. Vol. II: Diophantine analysis*, Chelsea Publishing Co., New York, 1966.

[8] Tim Dokchitser, *Computing special values of motivic L-functions*, Experiment. Math. **13** (2004). `http://projecteuclid.org/euclid.em/1090350929`.

[9] Andrej Dujella, *History of elliptic curves rank records.* `http://web.math.pmf.unizg.hr/~duje/tors/rankhist.html`.

[10] Neal Koblitz, *Introduction to elliptic curves and modular forms*, Second, Graduate Texts in Mathematics, vol. 97, Springer-Verlag, New York, 1993.

[11] V. A. Kolyvagin, *Finiteness of* $E(\mathbf{Q})$ *and* $SH(E, \mathbf{Q})$ *for a subclass of Weil curves*, Izv. Akad. Nauk SSSR Ser. Mat. **52** (1988).

[12] Álvaro Lozano-Robledo, *Elliptic curves, modular forms, and their L-functions*, American Mathematical Society, Providence, RI; Institute for Advanced Study (IAS), Princeton, NJ, 2011.

[13] Joseph H. Silverman and John Tate, *Rational points on elliptic curves*, Undergraduate Texts in Mathematics, Springer-Verlag, New York, 1992.

[14] W. A. Stein et al., *Sage Mathematics Software*, The Sage Development Team, 2015. `http://www.sagemath.org`.

[15] Richard Taylor and Andrew Wiles, *Ring-theoretic properties of certain Hecke algebras*, Ann. of Math. (2) **141** (1995).

[16] J. B. Tunnell, *A classical Diophantine problem and modular forms of weight* 3/2, Invent. Math. **72** (1983).

[17] Andrew Wiles, *Modular elliptic curves and Fermat's last theorem*, Ann. of Math. (2) **141** (1995).