CONGRUENT NUMBERS AND ELLIPTIC CURVES

JIM BROWN

Abstract. In this short paper we consider congruent numbers and how they give rise to elliptic curves. We will begin with very basic notions before moving into the world of elliptic curves. However, the entire paper is meant to be appropriate for an undergraduate audience. For the undergraduate with no abstract algebra experience it may be wise to skip the proofs. This paper owes a great debt to Koblitz’s wonderful treatment of the subject in [3].

1. Congruent numbers

One of the traits that sets number theory apart from many other branches of mathematics is the fact that many of the most difficult problems are very easy to state. In fact, the statement of many of these problems can be understood by a student in a high school mathematics class. The problem this paper focuses on is the congruent number problem.

Definition 1.1. An integer \( N \) is a congruent number if there exists a right triangle with rational sides so that the area of the triangle is \( N \).

Example 1.2. The number \( N = 6 \) is a congruent number as one sees by considering the \( 3 - 4 - 5 \) triangle.

The problem we are interested in is determining all possible congruent numbers. The natural place to begin is to attempt to classify all right triangle with integer sides.

Theorem 1.3. Let \( X, Y, \) and \( Z \) be integers and sides of a right triangle with \( \gcd(X, Y, Z) = 1 \). Then there exists \( m, n \in \mathbb{N} \) so that \( X = 2mn \), \( Y = m^2 - n^2 \) and \( Z = m^2 + n^2 \). Conversely, any \( m, n \in \mathbb{N} \) define a right triangle defining \( X, Y, \) and \( Z \) the same way.

Proof. It is clear that given \( m \) and \( n \) we obtain a right triangle with integer sides using the given formulas. We need to show that given a right triangle with integer sides \( X, Y, \) and \( Z \) that we can find such an \( m \) and \( n \). Observe that we have \( X^2 + Y^2 = Z^2 \) by the Pythagorean

Key words and phrases. Congruent numbers, elliptic curves.
theorem. Suppose $X$ and $Y$ are both odd. This implies that $Z^2 \equiv 2 \pmod{4}$. However, the squares modulo 4 are 0 and 1. Thus it must be that $X$ or $Y$ is even. Assume without loss of generality that $X$ is even so that $\frac{X}{2}$ is an integer. Write

$$
\left( \frac{X}{2} \right)^2 = \left( \frac{Z}{2} \right)^2 - \left( \frac{Y}{2} \right)^2 = \left( \frac{Z - Y}{2} \right) \left( \frac{Z + Y}{2} \right).
$$

If $p$ is a prime that divides $\frac{X}{2}$, then $p^2 \mid \left( \frac{X}{2} \right)^2$. Since $p$ is prime, we have that $p \mid \left( \frac{Z - Y}{2} \right)$ or $p \mid \left( \frac{Z + Y}{2} \right)$. Note that $p$ cannot divide both since $\gcd(X, Y, Z) = 1$. Thus we obtain that $p^2 \mid \left( \frac{Z - Y}{2} \right)^2$ or $p^2 \mid \left( \frac{Z + Y}{2} \right)^2$.

Running through all the primes that divide $\frac{X}{2}$, we see that we can write

$$
\left( \frac{X}{2} \right)^2 = m^2n^2
$$

where $m$ is composed of those primes that divide $\left( \frac{Z - Y}{2} \right)$ and $n$ is composed of those primes that divide $\left( \frac{Z + Y}{2} \right)$. This gives that $X = 2mn$, $Y = m^2 - n^2$ (assuming without loss of generality that $m > n$) and $Z = m^2 + n^2$, as desired.

This theorem allows us to generate all congruent numbers that arise from integer sided right triangles. For example, we have the following table:

**Table 1. Congruent numbers from Pythagorean triples**

<table>
<thead>
<tr>
<th>m</th>
<th>n</th>
<th>X</th>
<th>Y</th>
<th>Z</th>
<th>N</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>1</td>
<td>4</td>
<td>3</td>
<td>5</td>
<td>6</td>
</tr>
<tr>
<td>3</td>
<td>1</td>
<td>6</td>
<td>8</td>
<td>10</td>
<td>24</td>
</tr>
<tr>
<td>3</td>
<td>2</td>
<td>12</td>
<td>5</td>
<td>13</td>
<td>30</td>
</tr>
<tr>
<td>4</td>
<td>1</td>
<td>8</td>
<td>15</td>
<td>17</td>
<td>60</td>
</tr>
<tr>
<td>4</td>
<td>3</td>
<td>24</td>
<td>7</td>
<td>25</td>
<td>84</td>
</tr>
<tr>
<td>4</td>
<td>2</td>
<td>16</td>
<td>12</td>
<td>20</td>
<td>96</td>
</tr>
<tr>
<td>5</td>
<td>1</td>
<td>10</td>
<td>24</td>
<td>26</td>
<td>120</td>
</tr>
<tr>
<td>5</td>
<td>4</td>
<td>40</td>
<td>9</td>
<td>41</td>
<td>180</td>
</tr>
</tbody>
</table>

Of course, we want to deal with triangles with rational sides as well. Suppose we have a right triangle with sides $X, Y, Z \in \mathbb{Q}$ and congruent number $N$. It is easy to see that we can clear denominators and obtain a right triangle with integers sides and congruent number $a^2N$ where $a$ is the least common multiple of the denominators of $X$ and $Y$. Thus, we can go from a right triangle with rational sides to a right triangle with integer sides and a new congruent number that is divisible by a square. Conversely, given a right triangle with integer sides $X, Y$, and $Z$ and congruent number $N = a^2N_0$, we can form a right triangle with
rational sides and congruent number $N_0$ by merely dividing $X$ and $Y$ by $a$.

**Example 1.4.** Consider the $40 - 9 - 41$ triangle given by $m = 5$ and $n = 4$. This triangle has area $180 = 6^2 5$. Thus, $5$ is a congruent number given by a triangle with sides $\frac{3}{2}$, $\frac{20}{3}$, and $\frac{41}{6}$.

Some further examples are given in the following table.

**Table 2.** Congruent numbers from rational right triangles

<table>
<thead>
<tr>
<th>$X$</th>
<th>$Y$</th>
<th>$Z$</th>
<th>$N$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$3/2$</td>
<td>$20/3$</td>
<td>$41/6$</td>
<td>$5$</td>
</tr>
<tr>
<td>$4/9$</td>
<td>$7/4$</td>
<td>$65/36$</td>
<td>$14$</td>
</tr>
<tr>
<td>$4$</td>
<td>$15/2$</td>
<td>$17/2$</td>
<td>$15$</td>
</tr>
<tr>
<td>$7/2$</td>
<td>$12$</td>
<td>$25/2$</td>
<td>$21$</td>
</tr>
<tr>
<td>$4$</td>
<td>$17/36$</td>
<td>$145/36$</td>
<td>$34$</td>
</tr>
<tr>
<td>$28/9$</td>
<td>$5$</td>
<td>$53/9$</td>
<td>$70$</td>
</tr>
</tbody>
</table>

This method allows us to use the Pythagorean triples given in Theorem 1.3 to produce congruent numbers arising from triangles with rational sides. The difficulty is not in producing lots and lots of congruent numbers, the difficulty is proving that a given number is not congruent. Using the method described thus far, if we cannot find a triangle with area $N$, it does not mean $N$ is not congruent. It may just be that we have not looked hard enough to find the triangle. For example, the integer $157$ is a congruent number. However, the simplest triangle giving area $157$ has sides given by

$$X = \frac{6803298487826435051217540}{411340519227716149383203}, \quad Y = \frac{411340519227716149383203}{21666555693714761309610}.$$  

Clearly we are going to need a new method to solve this problem.

2. From congruent numbers to elliptic curves

Let $N$ be a congruent number given by a right triangle with sides $X, Y, Z \in \mathbb{Q}$, i.e., we have

$$X^2 + Y^2 = Z^2$$

and

$$\frac{1}{2}XY = N.$$

If we multiply equation (2) by 4 and add and subtract it from equation (1) we obtain the equations

$$(X + Y)^2 = Z^2 + 4N$$
and

\[(X - Y)^2 = Z^2 - 4N\]

i.e., we have equations

(3) \[\left(\frac{X + Y}{2}\right)^2 = \left(\frac{Z}{2}\right)^2 + N\]

and

(4) \[\left(\frac{X - Y}{2}\right)^2 = \left(\frac{Z}{2}\right)^2 - N.\]

Multiplying equations (3) and (4) together we obtain

\[\left(\frac{X^2 - Y^2}{4}\right)^2 = \left(\frac{Z}{2}\right)^4 - N^2.\]

Thus, a rational right triangle with congruence number \(N\) produces a rational solution to the equation

(5) \[v^2 = u^4 - N^2,\]

namely \(v = \left(\frac{X^2 - Y^2}{4}\right)\) and \(u = \left(\frac{Z}{2}\right)\). Multiplying equation (5) by \(u^2\) we obtain

\[(uv)^2 = u^6 - N^2u^2.\]

If we set \(x = u^2 = \left(\frac{Z}{2}\right)^2\) and \(y = uv = \frac{Z(X^2 - Y^2)}{8}\), then we find that a rational right triangle with congruence number \(N\) produces a rational solution to the equation

(6) \[E_N : y^2 = x^3 - N^2x.\]

This curve is an example of type of curve known as an elliptic curve. We will come back to these curves in a more general setting in the next section. For now we have the following result stating that this process can be reversed and we can use certain points on elliptic curves of the form \(E_N\) to show that \(N\) is a congruent number.

**Proposition 2.1.** Let \((x, y)\) be a point with rational coordinates on the curve \(E_N\). Suppose \(x\) satisfies:

1. \(x\) is the square of a rational number
2. \(x\) has even denominator
3. the numerator of \(x\) is relatively prime to \(N\)

Then there exists a right triangle with area \(N\) and rational sides where the sides are given by \(X = \sqrt{x} + \sqrt{N} - \sqrt{x - N}, Y = \sqrt{x} + \sqrt{N} + \sqrt{x - N}\) and \(Z = 2\sqrt{x}\).
To prove this proposition one works backwards through the equations used to find \( E_N \) to get back to the original equations. It is left as an exercise to the curious reader.

3. Elliptic curves

In this section we gather some basic results on elliptic curves. We will return to the specific case of \( E_N \) in the next section.

**Definition 3.1.** An elliptic curve over \( \mathbb{Q} \) is a nonsingular curve of the form

\[
E : y^2 = x^3 + ax^2 + bx + c
\]

where \( a, b, c \in \mathbb{Z} \).

We say a point \( P = (x, y) \) is a point on \( E \) if it satisfies the equation defining \( E \). The set of all points \( P \) with \( x, y \in \mathbb{Q} \) is denoted by \( E(\mathbb{Q}) \).

What makes elliptic curves special is that given two points \( P, Q \in E(\mathbb{Q}) \) one can define an addition \( \oplus \) on \( E(\mathbb{Q}) \) so that \( P \oplus Q \in E(\mathbb{Q}) \). In fact, this addition makes \( E(\mathbb{Q}) \) into an abelian group! We can view this addition geometrically. The naive version would be to define the point \( P \oplus Q \) as the third point of intersection \( R \) of the line through \( P \) and \( Q \) with \( E \). However, if we define addition this way we do not get that addition is associative! For example, consider the points \( P_1 = (-2, 8), P_2 = (6, 0), \) and \( P_3 = (0, 0) \) on the curve \( E_6 \). One calculates that under this definition of addition one has \( (P_1 \oplus P_2) \oplus P_3 = (12, -36) \) and \( P_1 \oplus (P_2 \oplus P_3) = (12, 36) \). Instead, we define addition by taking the point \( R \) as above and drawing a vertical line through \( R \). This will hit \( E \) at another point which we define to be \( P \oplus Q \).

![Figure 1. Graphical representation that on \( E_6 \) one has \( P \oplus Q = (12, 36) \) for \( P = (-3, 9) \) and \( Q = (0, 0) \).](image-url)
Note that the identity of the group is the “point at infinity”. For those not familiar with projective geometry, just think of this as a point off the page obtained when you follow a vertical line to infinity. We will denote this point by $0_E$.

To see that the point $P \oplus Q$ actually has coordinates in $Q$, we work out the explicit formulas for $x(P \oplus Q)$ and $y(P \oplus Q)$. Let $P = (x(P), y(P))$, $Q = (x(Q), y(Q))$ and $P \oplus Q = (x(P \oplus Q), y(P \oplus Q))$. Observe that the line through $P$ and $Q$ can be written in the form $y = mx + b$ with $m = \frac{y(P) - y(Q)}{x(P) - x(Q)}$ if $P \neq Q$ and $m = \frac{f'(x(P))}{2y(P)}$ if $P = Q$ where $f(x) = x^3 + ax^2 + bx + c$. The value of $x(P \oplus Q)$ is the third root of the cubic

$$f(x) - (mx + b)^2.$$

The sum of the roots is equal to the negative of the coefficient of $x^2$, so

$$x(P) + x(Q) + x(P \oplus Q) = -(a - m^2).$$

Thus,

$$x(P \oplus Q) = -x(P) - x(Q) - a + m^2.$$

The $y$-value is the negative of the $y$-value of the third point of intersection of the line and the curve, so

$$y(P \oplus Q) = y(P) - m(x(P) - x(Q)).$$

It is important to keep in mind this addition is NOT component-wise addition. The following example was computed using SAGE.

**Example 3.2.** Consider the elliptic curve $E_6 : y^2 = x^3 - 36x$. Let $P = (-2, 8)$ and $Q = (6, 0)$. It is easy to check these are each points on $E_6$ by plugging in the values for $x$ and $y$. We then have $2 \ast Q = 0_E$, $P \oplus Q = (-3, 9)$, and $5 \ast P = \left(-\frac{10749002978}{2015740609}, \frac{394555797978644}{90507612273}\right)$.

We can consider all the points $P \in E(\mathbb{Q})$ so that $M \ast P = 0_E$ for some $M \in \mathbb{Z}$. For example, $Q$ in the previous example satisfied $2 \ast Q = 0_E$. The set of such points is a group called the group of torsion points of $E(\mathbb{Q})$ and we write $E(\mathbb{Q})_{\text{tors}}$. It turns out that there are only 15 possibilities for $E(\mathbb{Q})_{\text{tors}}$: $\mathbb{Z}/M\mathbb{Z}$ for $1 \leq M \leq 10$ or $M = 12$ or $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2M\mathbb{Z}$ for $1 \leq M \leq 4$. This is a very deep result of Mazur ([4], [5]). The important point for us is that the torsion subgroup is finite and we have a pretty good grasp on it. The full structure of $E(\mathbb{Q})$ is given by Mordell’s theorem.

**Theorem 3.3.** (Mordell’s theorem) The group $E(\mathbb{Q})$ is given by

$$E(\mathbb{Q}) \cong E(\mathbb{Q})_{\text{tors}} \oplus \mathbb{Z}^r$$

where $r$ is an integer called the rank of the elliptic curve.
For our purposes, the thing to take from this theorem is that the rank of the elliptic curve tells us about non-torsion points on the curve. In particular, if one has a point that is not in $E(\mathbb{Q})_{\text{tors}}$, then one has $r > 0$ and there must be infinitely many points not in $E(\mathbb{Q})_{\text{tors}}$.

4. The elliptic curve $E_N$

We now specialize to the case of elliptic curves of the form $E_N$. In this case, it can be shown that

$$E_N(\mathbb{Q})_{\text{tors}} = \{0_E, (0, 0), (\pm N, 0)\}. \tag{7}$$

Note that the nonzero points here all have order 2. We have the following important proposition relating congruent numbers to ranks of elliptic curves.

**Proposition 4.1.** The integer $N$ is a congruent number if and only if $E_N(\mathbb{Q})$ has nonzero rank $r$.

**Proof.** Recall we are interested only in square-free $N$. Suppose that $N$ is a congruent number. We have already shown that this produces a point in $E_N(\mathbb{Q})$ with $x$-coordinate that is a nonzero square. (In fact, it was given by $\binom{Z}{2}$ for $Z$ the hypothenuse of the triangle with area $N$.) However, the $x$-coordinates of the nontrivial torsion points are 0 and $\pm N$. Thus, we must have the point produced is not a torsion point and hence we have that $E_N$ has nonzero rank.

Conversely, suppose we have a point $P \in E(\mathbb{Q})$ of infinite order. Observe that since $P$ is not of order 2, we can use the addition formula to obtain that $2 \ast P$ is a point of infinite order with $x$-coordinate given by

$$x(2 \ast P) = \frac{(x(P) + N^2)^2}{(2y(P))^2}.$$ 

This allows us to apply Proposition 2.1 to conclude $N$ is a congruent number. □

With this proposition we have reduced the problem of determining if $N$ is a congruent number to determining the rank of the elliptic curve $E_N$. Unfortunately, determining the rank of an elliptic curve is a very difficult problem. We need to introduce a function attached to $E_N$ called an $L$-function. Before we do this, we need to review some abstract algebra. For those who have taken abstract algebra and are familiar with finite fields, the following very rough paragraph can safely be skipped.
Let $p$ be a prime number. Given any integer $n$, we can consider the remainder when we divide $n$ by $p$. We can write

$$n = pq + \overline{n}$$

where $q \in \mathbb{Z}$ and $0 \leq \overline{n} < p$. It turns out we can add, subtract, multiply, and divide these remainders. Each time, we just consider the remainder upon division by $p$.

**Example 4.2.** Let $p = 5$. If we divide 19 by $p$ we get a remainder of 4, so $\overline{19} = \overline{4}$. Similarly, $\overline{27} = \overline{2}$. If we want to add these, we see that $\overline{19} + \overline{27} = \overline{4} + \overline{2} = \overline{6} = \overline{1}$. Each time, we just remove multiples of $p$ until the answer falls in the range $0 \leq \overline{n} < p - 1$.

The set of all remainders with this arithmetic structure is denoted by $\mathbb{F}_p$. Note that $\# \mathbb{F}_p = p$.

We now can consider a new elliptic curve defined over $\mathbb{F}_p$ instead of over $\mathbb{Q}$ where the elliptic curve is defined by

$$E_N : y^2 = x^3 - N^2 x.$$  

(Actually, this is only an elliptic curve at primes $p$ so that $p \nmid 2N$. However, we ignore this restriction here.) The group of points $E_N(\mathbb{F}_p)$ is a finite group that we can determine by just plugging in the $p^2$ possible points. Set $a_p = p + 1 - \#E_N(\mathbb{F}_p)$. We define the $L$-function of $E_N$ by

$$L(s, E_N) = \prod_{p \text{ prime}} \left(1 - a_p p^{-s} + p^{1-2s}\right)^{-1}$$

where $s \in \mathbb{C}$. Note that this is not the correct definition for those $p \mid 2N$, but again we ignore this complication. We also note that this function is not a priori defined on all of $\mathbb{C}$. However, it does have analytic continuation to $\mathbb{C}$ and we make use of this fact here without saying more. The weak form of the Birch and Swinnerton-Dyer conjecture (BSD) can now be stated.

**Conjecture 4.3.** (BSD) One has $L(1, E_N) = 0$ if and only if $r > 0$ where $r$ is the rank of $E_N$.

The Birch and Swinnerton-Dyer conjecture actually predicts that the order of vanishing of $L(1, E_N)$ should be exactly the rank of $E_N$. In fact, it can be made more precise to give subtle arithmetic information, but we omit that here as it requires significantly more background the the target audience will have. If we assume BSD is true, then we have the following proposition.

**Proposition 4.4.** (Assuming BSD) The integer $N$ is a congruent number if and only if $L(1, E_N) = 0$. 

The work of [2], [8], [6], and [1] show that for $E_N$ one has if $r > 0$ then $L(1, E) = 0$. (In fact, this is true of any elliptic curve with complex multiplication.) The other direction is still an open problem. However, Tunnell was able to prove the following theorem which assuming the validity of BSD reduces the problem of determining if $N$ is a congruent number to comparing the orders of simple finite sets.

**Theorem 4.5.** ([7]) If $N$ is square-free and odd (respectively even) and $N$ is the area of a rational right triangle, then

$$
\#\{x, y, z \in \mathbb{Z} \mid N = 2x^2 + 2y^2 + 32z^2\} = \frac{1}{2}\#\{x, y, z \in \mathbb{Z} \mid N = 2x^2 + y^2 + 8z^2\}
$$

(respectively

$$
\#\{x, y, z \in \mathbb{Z} \mid \frac{N}{2} = 4x^2 + y^2 + 32z^2\} = \frac{1}{2}\#\{x, y, z \in \mathbb{Z} \mid \frac{N}{2} = 4x^2 + y^2 + 8z^2\}
$$

If BSD is true for $E_N$, then the equality implies $N$ is a congruent number.

**References**


Department of Mathematics, The Ohio State University, Columbus, OH 43210

E-mail address: jimlb@math.ohio-state.edu