

Alex, I will take congruent numbers for one million
dollars please

Jim L. Brown
The Ohio State University
Columbus, OH 43210
jimlb@math.ohio-state.edu

One of the most alluring aspects of number theory is the relative ease with which some of the deepest and most difficult problems can be stated. For example, the twin prime conjecture states that there are infinitely many primes p so that $p+2$ is also a prime. While anyone who is familiar with basic arithmetic can understand the statement of the conjecture, as of yet there is not a single person who knows how to prove it! It is often the case that studying such seemingly simple problems leads to very deep mathematics that at first is hard to imagine is related.

The problem of interest here is of finding an efficient method of determining if a positive integer is the area of a right triangle with rational side lengths. The number 6 is an example of such a number given by the 3-4-5 triangle. Less obvious is the fact that 5 is also an example given by the triangle with side lengths $3/2, 20/3, 41/6$. We say a positive integer N is a *congruent number* if it is the area of a right triangle with rational side lengths. Thus, 5 and 6 are examples of congruent numbers. We will shortly see how the study of such numbers leads into the fascinating world of elliptic curves. Of course the natural starting place with which to study areas of right triangles is in studying right triangles!

We say positive integers X, Y and Z form a *Pythagorean triple* if X, Y and Z are the sides of a right triangle. If $\gcd(X, Y, Z) = 1$ we say they are a *primitive Pythagorean triple*. As a starting point in our study of congruent numbers we have the following theorem classifying all primitive Pythagorean triples.

THEOREM 1: Let X , Y , and Z be a primitive Pythagorean triple. Then there exist positive integers m and n ($m > n$) so that $X = m^2 - n^2$, $Y = 2mn$, and $Z = m^2 + n^2$. Conversely, any positive integers m and n with $m > n$ define a right triangle using the given formulas.

Proof: It is not hard to see that given m and n we obtain a right triangle with integer sides using the given formulas. We need to show that given a primitive Pythagorean triple 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 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 Y is even so that $\frac{Y}{2}$ is an integer. Write

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

If p is a prime that divides $\frac{Y}{2}$, then $p^2 \mid \left(\frac{Y}{2}\right)^2$. Since p is prime, we have that $p \mid \left(\frac{Z-X}{2}\right)$ or $p \mid \left(\frac{Z+X}{2}\right)$. Note that p cannot divide both for if it did we would have $p \mid \left(\left(\frac{Z-X}{2}\right) + \left(\frac{Z+X}{2}\right)\right) = Z$ and $p \mid \left(\left(\frac{Z+X}{2}\right) - \left(\frac{Z-X}{2}\right)\right) = X$ which would contradict $\gcd(X, Y, Z) = 1$. Thus we obtain that $p^2 \mid \left(\frac{Z-X}{2}\right)^2$ or $p^2 \mid \left(\frac{Z+X}{2}\right)^2$. Running through all the primes that divide $\frac{Y}{2}$, we see that we can write $\left(\frac{Y}{2}\right)^2 = m^2 n^2$ where m is composed of those primes that divide $\left(\frac{Z+X}{2}\right)$ and n is composed of those primes that divide $\left(\frac{Z-X}{2}\right)$. This gives that $X = m^2 - n^2$, $Y = 2mn$ and $Z = m^2 + n^2$, as desired.

This theorem allows us to generate all congruent numbers that arise from integer sided right triangles. Some examples are given in Table 1.

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 area N . It is easy to see that we can clear denominators and obtain a right triangle with integers sides and area $a^2 N$ 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

Table 1: Congruent numbers from Pythagorean triples

m	n	X	Y	Z	N
2	1	4	3	5	6
3	1	6	8	10	24
3	2	12	5	13	30
4	1	8	15	17	60
4	3	24	7	25	84
4	2	16	12	20	96
5	1	10	24	26	120
5	4	40	9	41	180

is divisible by a square. Conversely, given a right triangle with integer sides X, Y , and Z and area $N = a^2 N_0$, we can form a right triangle with rational sides and area N_0 by merely dividing X and Y by a . Thus, it is enough to study positive integers N that are square-free when studying congruent numbers. For example, consider the 8-15-17 triangle with area $60 = 2^2 \cdot 3 \cdot 5$. From the previous discussion we see that 15 is a congruent number given by the triangle with sides 4, $15/2$, $17/2$. Some further examples are given in Table 2.

This method allows us to use the Pythagorean triples given in Theorem 1 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 determining if a given integer N is a congruent number. 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

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

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

Table 2: Congruent numbers from rational right triangles

X	Y	Z	N
3/2	20/3	41/6	5
4/9	7/4	65/36	14
4	15/2	17/2	15
7/2	12	25/2	21
4	17/36	145/36	34
28/9	5	53/9	70

Before we embark on a new method of attack, we note that we have yet to see why such an N is called a congruent number. The following theorem answers this question. It says that if N is a congruent number we obtain three squares of rational numbers that are congruent modulo N . The proof is left as an exercise to the curious reader.

THEOREM: Let N be a square-free positive integer. Let X, Y, Z be positive rational numbers with $X < Y < Z$. There is a 1-1 correspondence between right triangles with sides X, Y, Z and area N and numbers $x \in \mathbb{Q}$ so that $x, x + N, x - N$ are all squares of rational numbers.

Elliptic curves? Are you sure?

An elliptic curve, as the name suggests, is a special type of plane curve. What we mean by a *plane curve* C is the solution set of an equation $f(x, y) = 0$ where $f(x, y)$ is a polynomial in variables x and y . We say a point (x_0, y_0) is a *point on the curve* C if $f(x_0, y_0) = 0$. We say the point (x_0, y_0) is a *rational point on the curve* if (x_0, y_0) is a point on the curve and $x_0, y_0 \in \mathbb{Q}$. We will denote the set of rational points of the curve C by $C(\mathbb{Q})$. We say the curve is *smooth* if the partial derivatives of $f(x, y)$ with respect to x and y do not simultaneously vanish at any point on the curve. For example the circle of

radius 1 is a smooth plane curve given by the polynomial $f(x, y) = x^2 + y^2 - 1$.

An elliptic curve defined over a field K (you can take $K = \mathbb{Q}$ here if you like) is a smooth plane curve E defined by the polynomial

$$f(x, y) = y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_5$$

where the a_i all lie in K . We will also want to include a “point at infinity”, but we will come back to this later. The only elliptic curves we are interested in are the ones defined by the polynomial $f(x, y) = y^2 - x^3 + N^2x$ for N a positive square-free integer. We will often denote this elliptic curve by E_N and write

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

This is all fine, but what does it have to do with congruent numbers? Define the set \mathcal{A}_N by

$$\mathcal{A}_N = \left\{ (X, Y, Z) \in \mathbb{Q}^3 : \frac{1}{2}XY = N, X^2 + Y^2 = Z^2 \right\}.$$

It is easy to see that N is a congruent number if and only if \mathcal{A}_N is not the empty set. The important point is that there is a bijection between \mathcal{A}_N and the set

$$\mathcal{B}_N = \{(x, y) \in \mathbb{Q}^2 : y^2 = x^3 - N^2x, y \neq 0\}$$

given by functions

$$f(X, Y, Z) = \left(-\frac{NY}{X+Z}, \frac{2N^2}{X+Z} \right)$$

and

$$g(x, y) = \left(\frac{N^2 - x^2}{y}, -\frac{2xN}{y}, \frac{N^2 + x^2}{y} \right).$$

This shows that if we can find a point $P = (x(P), y(P)) \in E_N(\mathbb{Q})$ with $y(P) \neq 0$, then we have that N is a congruent number! Thus, it might actually be worth our time to study rational points on the elliptic curves E_N .

So what makes us think that studying rational points on E_N will lead to any new information? It turns out that elliptic curves are very special types of curves. We can define an operation \oplus so that if $P, Q \in E_N(\mathbb{Q})$ then $P \oplus Q \in E_N(\mathbb{Q})$. In fact \oplus is not any old operation, it makes the set $E_N(\mathbb{Q})$ into an abelian group!

Before we can define the addition on $E_N(\mathbb{Q})$, we need to introduce the “point at infinity”. For the reader familiar with stereographic projection, the point at infinity can be taken to be the north pole of the sphere. Even better, if you are familiar with projective geometry it is the point $(0 : 1 : 0)$. If both of those notions are foreign, you can think of the point at infinity as the point off of the page if you go in the y -direction forever. For an introduction to projective geometry geared to this setting consult [1].

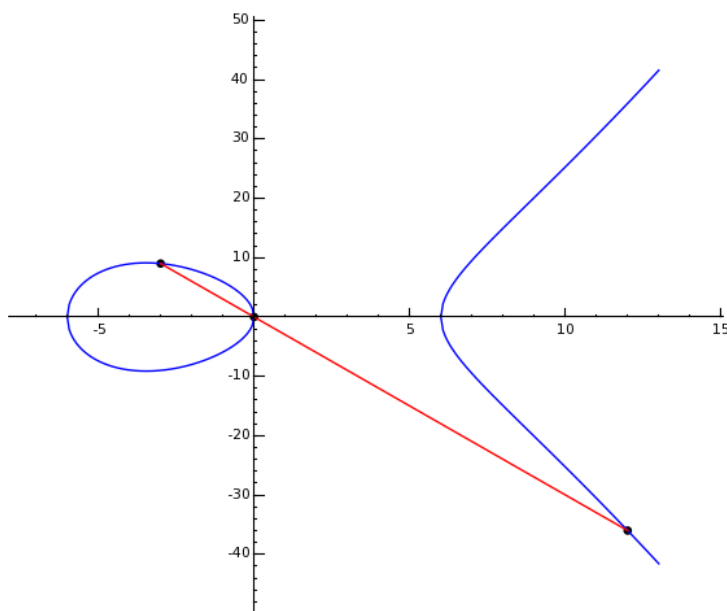


Figure 1: Graphical representation that on E_6 one has $P \boxplus Q = (12, -36)$ for $P = (-3, 9)$ and $Q = (0, 0)$.

The fact that the equation defining E_N is a cubic implies that any line

that intersects the curve must intersect it at exactly three points if we include the point at infinity as well and count a tangent as a double intersection point. This would lead one to guess that defining the point $P \oplus Q$ is as simple as setting it equal to the third intersection point of the line through P and Q . Unfortunately, defining addition in this way would miss the important property of associativity! You should check by drawing pictures that this definition of addition, call it \boxplus , is not associative. See Figure 1 for an illustration of the operation \boxplus .

What turns out to be the correct definition of $P \oplus Q$ is to take the third point of intersection R of the line through P and Q and the elliptic curve and reflect it over the x -axis as pictured in Figure 2.

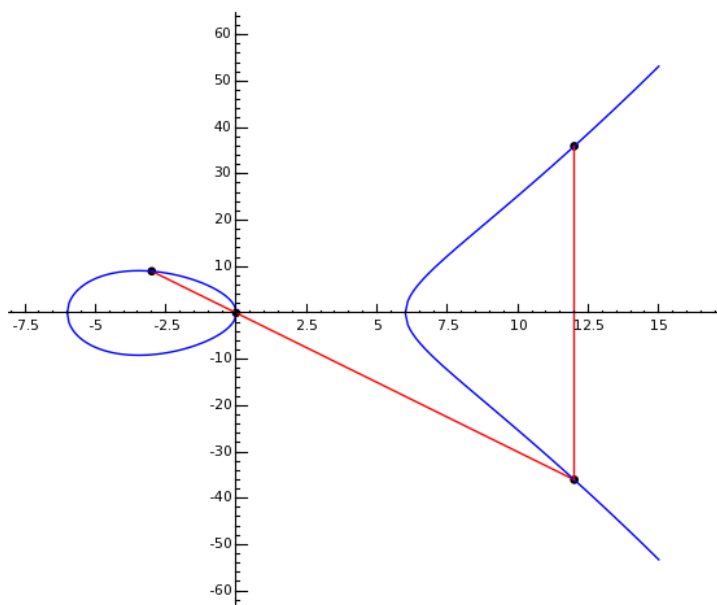


Figure 2: Graphical representation that on E_6 one has $P \oplus Q = (12, 36)$ for $P = (-3, 9)$ and $Q = (0, 0)$.

Note that what we are really doing is finding the point R and then taking another line through R and the point at infinity and taking the third inter-

section point with E_N as $P \oplus Q$. This makes it easy to see that the point at infinity acts as the identity element of the group. In the future we will often write 0_{E_N} for the point at infinity to reflect this fact. You should convince yourself with pictures that $P \oplus Q = Q \oplus P$, $P \oplus 0_{E_N} = P$, and if $P = (x, y)$, then $-P = (x, -y)$, i.e., $P \oplus (-P) = 0_{E_N}$. If you are really brave try to prove that the addition is associative as well. (Hint: colored pencils are very helpful!)

This method shows that given two points P and Q on E_N we get a third point $P \oplus Q$ on E_N . What we have not shown yet is given $P, Q \in E_N(\mathbb{Q})$ that $P \oplus Q \in E_N(\mathbb{Q})$, i.e., that the coordinates of $P \oplus Q$ are rational numbers. In order to show this we compute the coordinates of $P \oplus Q$ in terms of those of P and Q . Write $P = (x(P), y(P))$ and similarly for Q and $P \oplus Q$. Note that if we define R as above being the third intersection point of the line through P and Q with E_N , then $x(R) = x(P \oplus Q)$ and $y(R) = -y(P \oplus Q)$, so it is enough to determine $x(R)$ and $y(R)$ in terms of $x(P), x(Q), y(P)$ and $y(Q)$. We deal with the case $P \neq Q$ and leave the case of $P = Q$ as an exercise. Let ℓ be the line through P and Q , i.e., ℓ is the equation $y - y(P) = m(x - x(P))$ where $m = \frac{y(P) - y(Q)}{x(P) - x(Q)}$. Define

$$f(x) = x^3 - N^2x - (m(x - x(P)) + y(P))^2.$$

From the definition of ℓ we see that $f(x(P)) = f(x(Q)) = f(x(R)) = 0$. Since $f(x)$ is a degree three polynomial in x and we have three roots of $f(x)$ these are necessarily all the roots. Recall the following basic result from algebra.

THEOREM: Let $g(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0$. Let $\alpha_1, \dots, \alpha_n$ be the roots of $g(x)$. Then

$$-a_{n-1} = \sum_{i=1}^n \alpha_i.$$

This theorem allows us to conclude that

$$x(P) + x(Q) + x(R) = m^2.$$

Thus, $x(R) = m^2 - x(P) - x(Q)$. The fact that $P, Q \in E_N(\mathbb{Q})$ shows that $m, x(P), x(Q) \in \mathbb{Q}$ and so $x(P \oplus Q) = x(R) \in \mathbb{Q}$ as well. It remains to calculate $y(R)$. For this, we merely plug $y(R)$ in for y in the equation of ℓ giving

$$y(R) = m(x(R) - x(P)) + y(P).$$

Since everything on the right hand side of this equation is in \mathbb{Q} , so is $y(R)$ and hence $y(P \oplus Q) = -y(R) \in \mathbb{Q}$. This, combined with the properties mentioned earlier makes $E_N(\mathbb{Q})$ into an abelian group under the operation \oplus with identity the point at infinity.

EXAMPLE: Consider the elliptic curve E_6 . It is easy to see that the points $(0, 0)$ and $(\pm 6, 0)$ are rational points on this curve. We can use SAGE ([6]) to find other nontrivial points. Define the elliptic curve E_6 in SAGE with the command:

```
sage: E6 = EllipticCurve([-36,0])
```

To find points one uses the command:

```
sage: E6.point_search(10)
```

The 10 in this command is telling it how many points to search; essentially it is checking all points up to a certain “height”. The only thing we need to remember is that the bigger the number we put in, the longer the process takes. Staying under 20 is generally a good idea. Upon executing this command we receive a large amount of information. At this point all we are interested in are the points it gives us. These points will be in projective coordinates so some care is needed. The points in the xy -plane correspond to the points $(x : y : z)$ with $z \neq 0$. To convert them into xy -coordinates we merely divide each term by z . The first two entries are then our (x, y) point. Some points it gives us are $(-2 : 8 : 1)$, $(12 : 36 : 1)$, and $(50 : 35 : 8)$. Upon normalizing so $z = 1$ we get the (x, y) points $(-2, 8)$, $(12, 36)$, and $(25/4, 35/8)$. The point with $z = 0$ is the point at infinity, i.e., our identity element 0_{E_6} . We can now use SAGE to add any of these points for us.

```

sage: P1 = E6([-2, 8]); P2 = E6([12, 36]); P3 = E6([-6, 0])
sage: P1 + P2
(-6 : 0 : 1)
sage: 5 * P1
(-1074902978 : 394955797978664 : 1)
      2015740609 : 90500706122273
sage: 2 * P3
(0 : 1 : 0)

```

The notation $5P1$ is shorthand for the sum $P1 \oplus \cdots \oplus P1$ with five copies of $P1$. Note that $P3 \oplus P3 = 0_{E_N}$ as this will be important. You should compute a couple of these by hand to make sure you are comfortable working with the formulas derived above!

One million dollars...

It now remains to find a way to find rational points on E_N with y -coordinate non-zero or to at least ensure that such a point exists even if we cannot find it. This leads us to study the structure of the group $E_N(\mathbb{Q})$.

A point $P \in E_N(\mathbb{Q})$ is called a *torsion point* if there exists a nonzero integer m so that $mP = 0_{E_N}$. For example, the point $P3$ in the above example is a torsion point with $m = 2$. The set of all such points forms a subgroup of $E_N(\mathbb{Q})$ called the torsion subgroup and denoted by $E_N(\mathbb{Q})_{\text{tors}}$. It turns out by work of Mazur ([4], [5]) that the torsion group of a general elliptic curve is not so hard to understand. In our case, it is even easier as we have the following theorem.

THEOREM 2: The torsion subgroup of $E_N(\mathbb{Q})$ is given by

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

The proof of this theorem is not difficult, but it is too long to include here. The interested reader is urged to consult [1] or [3] for an elementary proof. A simple calculation shows that the only points in $E_N(\mathbb{Q})$ with y -coordinate

equal to 0 are in $E_N(\mathbb{Q})_{\text{tors}}$, so if we can simply find a point that is not a torsion point we will be able to use the bijection between \mathcal{A}_N and \mathcal{B}_N to produce a triangle with rational sides and area N .

EXAMPLE: We use the results obtained thus far to show that 137 is a congruent number and find a triangle with area 137. Using SAGE as above we find that $(-\frac{3136}{25}, \frac{77112}{125}) \in E_{137}(\mathbb{Q})$. Theorem 2 gives that this point is not in $E_{137}(\mathbb{Q})_{\text{tors}}$ so 137 is indeed a congruent number. We apply the bijection between \mathcal{A}_{137} and \mathcal{B}_{137} to obtain a triangle with sides $\frac{1377}{280}$, $\frac{76720}{1377}$, $\frac{21565121}{385560}$ and area 137.

The definition of torsion point implies that if $P \in E_N(\mathbb{Q})$ is not a torsion point, then we have $\langle P \rangle = \{nP : n \in \mathbb{Z}\}$ is isomorphic to \mathbb{Z} as an abelian group. We say two non-torsion points P and Q in $E_N(\mathbb{Q})$ are *independent* if $Q \neq mP \oplus T$ for any $m \in \mathbb{Z}$ and any $T \in E_N(\mathbb{Q})_{\text{tors}}$, i.e., if Q is not in the group generated by P and the torsion points. The number of independent points is the *rank* of the elliptic curve.

THEOREM (MORDELL-WEIL): $E_N(\mathbb{Q}) \cong E_N(\mathbb{Q})_{\text{tors}} \oplus \mathbb{Z}^r$ where here \oplus denotes a direct sum of abelian groups and r is the rank of the curve E_N .

Thus, we have turned the question of determining if N is a congruent number into the question of determining if the rank of E_N is positive. This is where the million dollars comes into play! First we need to define the L -function of the curve E_N .

We denote the finite field with p elements by \mathbb{F}_p and reduction of an element a modulo p by \bar{a} where p is a prime. If you are unfamiliar with finite fields, the element \bar{a} is just the remainder of a upon division by p . If we avoid the primes p where $p \mid 2N$, then the equation

$$\bar{E}_N : y^2 = x^2 - \bar{N}^2 x$$

defines an elliptic curve over \mathbb{F}_p . Since there are only finitely many pos-

sibilities for points (x_0, y_0) in $\overline{E}_N(\mathbb{F}_p)$, we can easily just check each possibility! Thus, it is not computationally difficult to determine the integers $a(p, E_N) = p + 1 - \#\overline{E}_N(\mathbb{F}_p)$. In fact, it can be shown that $a(p, E_N) = 0$ for all primes p with $p \equiv 3 \pmod{4}$. For $s \in \mathbb{C}$ with the real part of s larger than $3/2$ we define the L -function associated to E_N by

$$L(s, E_N) = \prod_{p \nmid 2N} (1 - a(p, E_N)p^{-s} + p^{1-2s})^{-1}.$$

Note that this function is not defined on all of \mathbb{C} . However, it can be analytically continued to the entire complex plane so we say no more about convergence here. Our interest in this function is the conjectural connection it has to the rank of the elliptic curve.

CONJECTURE (BIRCH AND SWINNERTON-DYER): The order of vanishing of $L(s, E_N)$ at $s = 1$ is precisely the rank of the elliptic curve E_N .

Thus, if we can show that $L(1, E_N) = 0$, then the rank of E_N must be positive and so we will have that there is a non-torsion point in $E_N(\mathbb{Q})$ and so N must be a congruent number! Unfortunately (or fortunately if you prove it!) this conjecture is one of the Clay Mathematics Institute's Millenium problems. This means if you prove or disprove this conjecture you will be awarded a million bucks! As you may suspect, this also means it is a very difficult problem.

Even though the function $L(s, E_N)$ seems to be a very complicated function, we can expand it out into a summation and then take finite approximations to it and obtain estimates as to whether it is zero or not at $s = 1$. This is built into SAGE as the command `E.Lseries(1)`. So we can, at least for small N , just work with the computer program SAGE to determine if N is a congruent number or not. However, the larger N gets the more difficult it becomes to work computationally with the elliptic curve E_N . Fortunately, there is a result (depending on the validity of the Birch and Swinnerton-Dyer conjecture) that reduces the problem to counting cardinality of relatively small

finite sets.

THEOREM 3: ([8]) 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

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

If the conjecture of Birch and Swinnerton-Dyer is true for E_N , then the equality implies N is a congruent number.

Thus, we have come full circle in our discussion of congruent numbers. We began with an innocent looking problem about areas of right triangles with rational side lengths. We then saw how elliptic curves arise naturally in the study of congruent numbers. From here we saw that a million dollar open conjecture actually arises in the study of congruent numbers. Finally, we see that if this million dollar conjecture is true, determining if a number is a congruent number comes down to determining the cardinality of a finite set, a simple counting problem. Thus, granting that someone will eventually prove the Birch and Swinnerton-Dyer conjecture we have found an efficient way to determine if N is a congruent number or not. Of course, Theorem 3 still leaves us in the position of being able to prove that N is the area of a right triangle with rational side lengths but having no idea what those side lengths are! Thus, even granting the validity of a million dollar conjecture there is still work to be done to give a satisfactory conclusion to the study of congruent numbers.

References

- [1] J. Brown, Congruent numbers and elliptic curves, <http://www.math.ohio-state.edu/~jimlb/congruentnumberslong.pdf>

(2007) 1–26.

- [2] J. Chahal, Congruent numbers and elliptic curves, *Amer. Math. Monthly* **113** Vol 4 (2006), 308–317.
- [3] N. Koblitz, *Introduction to Elliptic Curves and Modular Forms*, Springer GTM 97, 1993.
- [4] B. Mazur, Modular curves and the Eisenstein ideal, *IHES Publ. Math.* **47** (1978), 33–186.
- [5] B. Mazur, Rational isogenies of prime degree, *Invent. Math.* **44** (1978), 129–162.
- [6] W. Stein, SAGE: *Software for Algebra and Geometry Exploration*, <http://modular.math.washington.edu/sage>.
- [7] W. Stein, *The congruent number problem: A thousand year old unsolved problem*, <http://modular.math.washington.edu/simuw06/notes/notes/index.html>.
- [8] J. Tunnell, A classical Diophantine problem and modular forms of weights $3/2$, *Invent. Math.* **72** (1983), 323–334.