The Congruent Number Problem

Graeme Brown

April 2, 2014

1 Introduction

In the eleventh century, the scholars of Emperor Frederic II challenged a well-known mathematical expert by the name of Leonardo Pisaro (better known as Fibonacci) to find 3 rational numbers whose squares form a common difference of 5. 6 was already known: consider the rational numbers $\frac{1}{2}$, $\frac{5}{2}$, $\frac{7}{2}$. Squaring these numbers gives $\frac{1}{4}$, $\frac{25}{4}$, $\frac{49}{4}$, three rational squares whose difference is six.

Not only did Leonardo supply them with an answer $(\frac{31}{12}, \frac{41}{12}, \frac{49}{12})$—indeed, if we square these three numbers we have $(\frac{961}{144}, \frac{1681}{144}, \frac{2401}{144})$ which it is easy to see have a common difference of $\frac{720}{144}$, or 5–but he went on to generalize the problem by asking how many integer numbers had this property in his 1225 book, *Liber Quadratorum*. The common difference, n, he gave a special name: congruum, from the Latin *congruere*, "to meet together". He gave an example not just of the case where n=5, but 7 as well $(\frac{113}{120}, \frac{337}{120}, \frac{467}{120})$, which you can verify for yourself. Further, he stated that no square can be a congruum, though he did so without proof. [1, 2]

Pisaro was not the first to ponder this problem. Diophantus' *Arithmetica* mentions the problem. The Arabs knew of congruent numbers, as can be found in tenth century manuscripts, and they went so far as so list that 5, 6, 14, 15, 21, 30, 34, 65, 70, 110, 154, 190—and even 10374—are all congruent numbers. It is thought that the Arabs might have leared of these numbers from the Hindus, who were already acquainted with the work of Diophantus.[3] The problem is also mentioned in 8th century Chinese manuscripts. [9, p.1]

After Pisaro's work, this problem lay dormant four hundred years. Pierre de Fermat contemplated the problem, along with his other more celebrated theorems, and it was during this time that it took on a new name: the congruent number problem.

2 Congruent Numbers and Right Triangles

Let's call our three special numbers r, s, and t, where $r < s < t$ and consider only those which have positive integer difference, $n > 0$. Then we have $s^2 - r^2 = n = t^2 - s^2$. Adding these two equalities produces $2n = t^2 - r^2 = (t-r)(t+r)$. Thus, $n = \frac{1}{2}(t-r)(t+r)$. If we let $t - r = a$ and $t + r = b$, then we notice our equation for n becomes $n = \frac{1}{2}ab$—the area for a right angle traingle! Indeed, we can find the hypoteneuse by the relation $a^2 + b^2 = c^2$:

$$a^2 + b^2 = (t-r)^2 + (t+r)^2$$

$$
\begin{aligned}
&= t^2 - 2tr + r^2 + t^2 + 2tr + r^2 \\
&= 2(t^2 + r^2) = 2(n + s^2 + s^2 - n) \\
&= (2s)^2
\end{aligned}
$$

Thus, one can form an association: $(r, s, t) \mapsto (t - r, t + r, 2s)$, and one can easily form a reverse association by simply recalling that $t - r = a$, $t + r = b$, and $c = 2s$: $(a, b, c) \mapsto (\frac{b-a}{2}, \frac{c}{2}, \frac{a+b}{2})$.

This translates the congruent problem into another problem. The existence of r, s, and t for the congruent number $n \in \mathbb{N} \Rightarrow n$ is the area of a right angle triangle with rational sides, $t - r$, $t + r$, and $2s$. [1, p.61]

Recall the earlier example for $n = 6$, $(\frac{1}{2}, \frac{5}{2}, \frac{7}{2})$. Using our translation, we can produce the triangle $(3, 4, 5)$, whose area we know is 6. Similarly, we see that our congruent numbers for 5 and 7, as presented earlier—namely, $(\frac{31}{12}, \frac{41}{12}, \frac{49}{12})$ and $(\frac{113}{120}, \frac{337}{120}, \frac{467}{120})$, respectively—work out to $(\frac{3}{2}, \frac{20}{3}, \frac{41}{6})$ and $(\frac{35}{12}, \frac{24}{5}, \frac{337}{60})$.

Now we see how easy it is to take any right angle triangle with integer area and rational sides and use the reverse transformation to find our desired rational squares in arithmetic progression.

Immediately, this allows us to consider only square free positive integers. Why? Suppose n is a congruent number. Let (a, b, c) be the corresponding right angle triangle. Multiply each side by a positive integer, m to produce a new triangle, (am, bm, cm). All these sides are rational, since a, b, and c are rational, so the area of this triangle will be a congruent number. This area is $\frac{1}{2}(am)(bm) = \frac{1}{2}abm^2 = nm^2$. Thus, if n is a congruent number, then any square multiplied by n is also a congruent number. In the hunt for congruent numbers, as soon as we find a congruent number, we can form the sequence $\{n, 4n, 9n, 16n, \ldots\}$.

Using this principle with just Fibonacci's results that 5 and 7 are congruent, along with the well-known example of 6 (the familiar 3,4, 5 triangle whose area is 6), we can construct a preliminary set of possible congruent numbers (for simplicity, we will stop at 126, but it is understood that this set is a subset of $\mathbb{N}$ and is therefore infinite):

$$C = \{5, 6, 7, 20, 24, 28, 45, 54, 63, 80, 96, 112, 125 \ldots\}$$

For the sake of good bookkeeping, let's consider also the numbers the Arabs found in our set, along with their square multiples too:

$$C = \{5, 6, 7, 14, 15, 20, 21, 24, 28, 30, 34, 45, 54, 56, 60, 63, 65, 70, 80, 84, 96, 110, 112, 120, 125, 126 \ldots\}$$

We should consider also the complement of this set:

$$H = \{1, 2, 3, 4, 8, 9, 10, 11, 12, 13, 16, 17, 18, 19, 22, 23, 25, 26, 27, 29, 31, 32, 33, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 46, 47, 48, 49, 50, 51, 52, 53, 55 \ldots\}$$

Our goal will be to search the set H for possibilities and either remove the number if we conclude it cannot be congruent, or else transfer it from H to C if we determine that the number is congruent. When $H = \varnothing$, with C containing all congruent numbers, then we have completed what Fibonacci began.

3 Fermat's Proofs

Pierre de Fermat contributed many things to the field of number theory. Based on his method of infinite descent, Fermat allows us to eliminate all square numbers from H. The proof is quite detailed and will be discussed briefly. For full reference, consult [4].

Fermat's proof is by contradiction. Suppose the set, S, of primitive right triangles with square area is not empty. Using definition of primitive triangles, Fermat chooses the least element in this set, the triangle T, corresponding to the Pythagoean triple $(a^2 - b^2, 2ab, a^2 + b^2)$, with $a > b$, $gcd(a, b) = 1$, and a and $a \not\equiv b$. This triangle has area $A = ab(a + b)(a - b)$, and since this area is a square, this requires a, b, $a + b$, and $a - b$ are all squares, since T is primitive. Using infinite descent, Fermat's proof shows us how we can construct a smaller triangle with a square area—contradicting that T is the least element in S. Thus, this assummption that S is nonempty is false and he therefore concludes that no triangle with square area can have rational sides.

This is a very powerful result. Fermat also proved that 2 is not congruent.[1, p.61] Putting this all together, we can rewrite our sets H as follows:

$$\begin{aligned} H = \{&3, 8, 10, 11, 12, 13, 17, 18, 19, 22, 23, 26, 27, 29, 31, 32, 33, 35, 37, 38, 39, 40, 41, 42, \\ &43, 44, 46, 47, 48, 50, 51, 52, 53, 55, 57, \ldots\} \end{aligned}$$

A beautiful picture is coming together. At this point, one can appeciate a subtle implication of our sets H and C: no triple of rational squares with an equal respective difference less than three will ever differ by a positive integer.

4 After Fermat...

Research in number theory after Fermat unearthed lots of information about congruent numbers. Mathematicians like Euler, Gauss, Genocchi, Bastien, Heegner, Gross, Stevens, Monsky, and Lagrange provided new ways to investigate numbers that allowed for broader criteria with which to decide which numbers are congruent and which are not.

There are several results, which can found in [2, p.41]. We will highlight a few, so as to further our goal to empty the set H and complete C.

A famous result of Heegner and Birch is that n is congruent if it is of the for $2p_3$, where p_3 is a prime $\equiv 3 \pmod{8}$. Such primes would be: 3, 11, 19, 43, 59, and thus we can transfer 6, 22, 38, 86, and 118 from C to H.

In 1975, Stevens found n is congruent if it is a prime $\equiv 5$ or $7 \pmod{8}$. This means that 5, 7, 23, 29, 31, 37, 47, 53, 61, 71, 79, 101, 103, 109, 119 can be trasfered to C.

Another result worth noting is that of B. Gross (1985), which states that n is congruent if it is of the form $\equiv 5, 6, or 7 \pmod{8}$ and has at most two prime factors with power 0 or 1. Using this criterion, we get can determine that the numbers 5, 6, 7, 13, 14, 15, 29, 31, 37, 39, 46, 47, 53, 55, 61, 62, 69, 71, 77, 79, 85, 86, 87, 93, 94, 95, 101, 103, 109, 111, 117, 118, 119 belong in C

There are also useful results that show when n is not congruent, which means we can further eliminate numbers from H. Bastien's result says that if $n = 2p$, where p is a prime $\equiv 9 \pmod{16}$, then n is congruent. Thus, we can eliminate 82 ($= 2 \cdot 41$, $41 \equiv 9(mod 16)$).

Genocchi provides four other powerful criteria to show n is congruent if:

- n is a prime $\equiv 3 \pmod 8$
- n is a product of two different primes both $\equiv 3 \pmod 8$
- $n = 2p$, where p $\equiv 5 \pmod 8$
- $n = 2pq$, where p, q $\equiv 5 \pmod 8$

Using Genocchi's results, we can also eliminate from H (in order of our list) 3, 11, 19, 43, 57, 59, 67, 83, 107; 33; 10, 26, 58, 74, 106, 122; (130 is the smallest number from the fourth criterion—and our rule was to track only numbers up to 126).

With these criteria and some careful bookkeeping, we can revise our sets:

$$\begin{aligned} C = \{&5, 6, 7, 13, 14, 15, 20, 21, 22, 23, 24, 28, 29, 30, 31, 34, 37, 38, 39, 45, 46, 47, 53, 54,\\ &55, 56, 60, 61, 62, 63, 65, 69, 70, 71, 77, 79, 80, 84, 85, 86, 87, 93, 94, 95, 96, 101,\\ &103, 109, 110, 111, 112, 117, 118, 119, 120, 125, 126\ldots\} \end{aligned}$$

$$\begin{aligned} H = \{&8, 12, 17, 18, 27, 32, 35, 40, 41, 42, 44, 48, 50, 51, 52, 59, 60, 63, 64, 65, 66, 68, 72, 73,\\ &75, 76, 78, 81, 88, 89, 90, 91, 92, 97, 98, 99, 100, 102, 104, 105, \ldots\} \end{aligned}$$

Given this new set, we return to our previous remark and make it stronger: no triple of rational squares with an equal respective difference less than five will ever differ by a positive integer.

5 Elliptic Curves: Finding a Sure Criterion

One can look for congruent numbers among the square-free, non-square positive integers. However, this is not an efficient method—if we can't find a rational side right triangle for a given area, n, then perhaps we haven't tried enough options. After all, there are an infinite number of possibilities!

Not all is lost. Just as we were able to equate Fibonacci's three-rational-square problem to that of rational-sided right angle triangles with integer area, we can take our transformation one step further, based on a derivation from [1, p.70].

Fix $n(\neq 0)$, with a, b, $c \in \mathbb{R} \setminus \{0\}$, corresponding to (a, b, c), a right angle triangle. Suppose that $a^2 + b^2 = c^2$ and $n = \frac{1}{2}ab$ describe two surfaces in $\mathbb{R}^3$. We wish to define the intersection of these surfaces.

Let $c = t + a$. Immediately note $\Rightarrow t \neq 0$, since otherwise $\Rightarrow c = a \Rightarrow b^2 = 0 \Rightarrow b = 0$, which is not allowed by the conditions we have declared. Now, $a^2 + b^2 = c^2 = t^2 + 2at + a^2$

$\Leftrightarrow b^2 = t^2 + 2at \Leftrightarrow 2at = b^2 - t^2$
And $n = \frac{1}{2}ab \Leftrightarrow a = \frac{2n}{b} \Rightarrow 2at = \frac{4nt}{b} = b^2 - t^2 \Leftrightarrow 4nt = b^3 - bt^2$
$\Leftrightarrow \frac{4n}{t^2} = \frac{b^3}{t^3} - \frac{b}{t} \Leftrightarrow \frac{4n^4}{t^2} = \frac{n^3b^3}{t^3} - \frac{n^2b}{t} \Leftrightarrow (\frac{2n^2}{t})^2 = (\frac{nb}{t})^3 - n^2(\frac{nb}{t})$

If we let $x = \frac{nb}{c-a}$ and $y = \frac{2n^2}{c-a}$, where $t = c - a$, then we form the association $(a, b, c) \mapsto (\frac{nb}{c-a}, \frac{2n^2}{c-a}) \in \mathbb{R}^2$. We define this new curve $E_n : y^2 = x^3 - n^2x$, an elliptic curve, and it is easily verified that any rational point on E_n can be mapped to a rational-sided right triangle according to the map $(x, y) \mapsto (\frac{x^2-n^2}{y}, \frac{2nx}{y}, \frac{x^2+n^2}{y})$.

Since n is congruent means a, b, c are rational, the congruent number problem now takes on a third form. We state that n is a congruent number $\Leftrightarrow \exists\ x, y \in \mathbb{Q}, y \neq 0$ for the associated elliptic curve, E_n.

As an example, consider the numbers Fibonacci found for $n = 5$, (3/2, 20/3, 41/6). Using our mapping, this produces the point $P = (\frac{25}{4}, \frac{75}{8}) \in E_n : y^2 = x^3 - 25x$. Now, by symmetry in our y term, $(\frac{25}{4}, -\frac{75}{8})$ is also on E_n. If we define the tangent line at P, then $x = \frac{25}{4}$ is a double root to E_n. If we let $y = mx + b$ represent the equation of the tangent line at P, then the intersection of this line with E_n defines a cubic, which has three roots. Since $\frac{25}{4}$ is already a double root, then by the qudratic equation $\Rightarrow \frac{25}{4}$ is also one part of a pair. The result is a new point $\in E_n$, say (x_1, y_1). One can take this point and reflect across the y-axis to get $(x_1, -y_1)$. We define this operation as $\oplus$ and call this new point $2P$.

One can continue in this fashion: join P to 2P by a line. By similar logic, there must exist a 3rd rational point on E_n. Reflect across the y-axis to produce $P \oplus 2P = 3P$. So, if n is a congruent number, then $\exists$ at least one rational nonzero solution $\Rightarrow E_n$ has an infinite number of rational nonzero solutions.

This has a wonderful implication. Since we can define a bijection between a nonzero rational point on E_n and a rational-sided right-angle triangle with area n (it is enough to consider only positive values of (a, b, c))[1, p.63-64], this in turn allows us, through the above mentioned mapping, $(x, y) \in E_n \mapsto (\frac{x^2-n^2}{y}, \frac{2nx}{y}, \frac{x^2+n^2}{y}) = (a, b, c) \mapsto (\frac{a-b}{2}, \frac{c}{2}, \frac{a+b}{2})$, to find an infinite number of square rational triples in arithmetic progression, n.

For example, consider the earlier example of $(\frac{1}{2}, \frac{5}{2}, \frac{7}{2}) \mapsto (3, 4, 5)$. Using the associated elliptic curve, $E_6 : y^2 = x^3 - 36x$ and the given mapping, we find $(3, 4, 5) \mapsto (12, 36)$. Calculating the slope of the tangent line at this point, we find it is $\frac{11}{2}$. Treating 12 as a double root, we find our third root of intersection to be $\frac{25}{4}$, which gives $y = \frac{35}{8}$, or $2P = (\frac{25}{4}, -\frac{35}{8})$. Now we can map this to a new rational-sided triangle via $(\frac{25}{4}, -\frac{35}{8}) \mapsto (\frac{(\frac{25}{4})^2-6^2}{(-\frac{35}{8})}, \frac{2(6)(\frac{25}{4})}{(-\frac{35}{8})}, \frac{(\frac{25}{4})^2+6^2}{(-\frac{35}{8})}) = (-\frac{7}{10}, -\frac{120}{7}, -\frac{1201}{70})$. Finally, ignoring the negative terms, we can use our mapping to translate this into a triple of rational points who squares differ by 6: $(\frac{7}{10}, \frac{120}{7}, \frac{1201}{70}) \mapsto (\frac{1151}{140}, \frac{1201}{140}, \frac{1249}{140})$.

Thus, via elliptic curves, we now have a tool to find an infinite number of rational triples whose squares differ by a number n, where n is congruent.

6 Tunnell's Theorem via Modularity and L-Functions

Elliptic curves equip us not just with a tool to provide infinite rational triples with common difference n, but also a possible once-and-for-all method to empty our set H and thus know all congruent numbers.

During the latter part of the twentieth century, mathematicians made great efforts to explore the properties of elliptic curves. Not only did this lead to the proof of Fermat's Last Theorem, it has given us the criteria we require to solve our problem. This is none other than the Taniyama-Shimura-Weil Conjecture, now known as Modularity Theorem, since it has been proved by Wiles, Tayler, Diamond, Conrad, and Breuil (2001).[5]

Full understanding of Modularity Theorem is well beyond the scope of this paper, but for the curious, one can consult [9], or [8] for an in-depth breakdown.

However, in order to appreciate Tunnell's Theorem, which gives us the criteria by which to at last complete our set C, we will look at some basic definitions to get an idea.

We have so far defined $E_n(\mathbb{Q})$, and Mordell's Theorem tells us for any elliptic curve, there are a finite number of points $\in E_n(\mathbb{Q})$ such that all of $E_n(\mathbb{Q})$ is generated by the above tangent-chord process discussed in each of these points. However, if we define $E_n(\mathbb{F}_p)$ instead, where $\mathbb{F}_p$ is a field of prime size, p, then it can be easily demonstrated that $E_n(\mathbb{F}_p)$ is a group, with a point at infinity as the identity (i.e. reflection in the y-axis).[6, p.334-335]

For each prime field, 3, 5, 7, 11, 13, 17, 19, ... we concern ourself with what is called the p-defect, a_p, the difference between p and the number of points in the group $E_n(\mathbb{F}_p)$, N_p.

It is easy to find N_p for a given curve, E_n when p is small. When p is large, one must use a computer, which was the focus of my summer research in 2013. Looking at the data, it is immediately apparent and easy to prove that for all primes of the form 3 (mod 4), $a_p = 0$—this is a consequence of the quadratic reciprocity law. (The proof can be found in [6, p. 352-356].) However, if $p \equiv 1 \pmod 4$, the picture becomes quite complicated.

Our goal is to find a pattern, or in other words to show that E_n is modular. Because of the tour-de-force proof that all elliptic curves are modular, we know we can expect one for the curves so defined by the congruent number problem.

As an example, consider a somewhat similar elliptic curve, $E : y^2 = x^3 + x$. A list of its a_p values, for $p = 5, 13, 17, 29, 37, 41, 53, \ldots$ is $2, -6, 2, 10, 2, 10, -14, \ldots$ One can notice that if $p \equiv 1 \pmod 4$ and $p = A^2 + B^2$, with A odd, then if $A \equiv 1 \pmod 4$, $N_p = p - 2A$. Otherwise, $N_p = p + 2A$. [6, p.350-1] Take, for example, $p = 5$. $p = 2^2 + 1$, so here $A = 1 \equiv 1 \pmod 4$, and we expect $N_5 = 5 - 2(1) = 3$, which means in turn that $a_p = 5 - 3 = 2$, which matches our results.

Determining a modularity pattern for our given curves, E_n is considerably more complicated, and is the basis of Tunnell's work. In general, it was shown by Hasse and Weil that $|E(\mathbb{F}_p)| = p + 1 - \alpha - \overline{\alpha}$, where $\alpha, \overline{\alpha}$ are complex conjugate numbers. One can generalize this over an extension of degree r and from this construct an L-function for E_n. [9, p.6]

In order to establish a modularity pattern for E_n, Tunnell had to assume the Birch-Swinnerton-Dyer conjecture to be true, which allowed him to define N_p for a given curve via its associated L-function: $L(E(\mathbb{F}_p), 1) = \prod_{p \geq 3}^{\infty} \frac{N_p}{p}$. Using nearly thirty years of results from the work of Coates, Wiles, Gross, Zagier, Rubin and Kolyvagin, then finally Modularity Theorem, Tunnel developed a criterion related to the modular form for E_n and the (assuming BSD true) fact that the associated L-function converges to zero $\Leftrightarrow$ n is a congruent number.[7, p.24]

7 The Set is Complete

We arrive then at a fourth and final equivalent problem. Assuming the Birch-Swinnerton-Dyer conjecture to be true, then n is a congruent number is equivalent to stating:

Given that n is congruent, define

$$\begin{aligned}
&A_n = |\{(x, y, z) \in \mathbb{Z}^3 | n = 2x^2 + y^2 + 32z^2\}| \\
&B_n = |\{(x, y, z) \in \mathbb{Z}^3 | n = 2x^2 + y^2 + 8z^2\}| \\
&C_n = |\{(x, y, z) \in \mathbb{Z}^3 | n = 8x^2 + 2y^2 + 64z^2\}| \\
&D_n = |\{(x, y, z) \in \mathbb{Z}^3 | n = 8x^2 + 2y^2 + 16z^2\}|
\end{aligned}$$

If n is odd, then $2A_n = B_n$
If n is even, then $2C_n = D_n$

Tunnell's criterion results from computing the number of points in a convergent L-function for E_n and is derived from the two forms of the associated theta function [9]. All that remains is for someone to prove the Birch-Swinnerton-Dyer conjuecture. Not only will that person allow us to once and for all know the complete set of congruent numbers, they would be $1 million richer, since it is one of the millenium problems.

Meanwhile, assuming that the Birch-Swinnerton-Dyer conjuecture is true, we can complete our quest by looking through what remains of H:

$$\begin{aligned}
H = \{&8, 12, 17, 18, 27, 32, 35, 40, 41, 42, 44, 48, 50, 51, 52, 59, 60, 63, 64, 65, 66, 68, 72, 73, \\
&75, 76, 78, 81, 88, 89, 90, 91, 92, 97, 98, 99, 100, 102, 104, 105, \ldots\}
\end{aligned}$$

8 is an even number, so we look for any integer solutions that satisfy $C_8 : 8 = 8x^2 + 2y^2 + 64z^2$ such that the number of solutions is half that of $D_8 : 8 = 8x^2 + 2y^2 + 16z^2$. Here, we find the same number of points for both, namely: $(\pm 1, 0, 0), (0, \pm 2, 0)$, i.e 4 points. This does not satisfy Tunnell's criterion, and so we eliminate 8 from H.

We find a similar result for 12, 17, 18, 27, 32, 35, and 40. But 41 works:

$A_{41} : 41 = 2x^2 + y^2 + 32z^2$ has solutions $(0, \pm 3, \pm 1)$, 4 solutions, while $B_{41} : 41 = 2x^2 + y^2 + 8z^2$ has 8 solutions: $(\pm 4, \pm 3, 0)$ and $(0, \pm 3, \pm 2)$. This satisfies Tunnell's criterion and thus 41 is a congruent number.

Continuing on in this fashion (a computer can do the work for us from here), we complete what we set out to show:

$H = \varnothing$

$$\begin{aligned}
C = \{&5, 6, 7, 13, 14, 15, 20, 21, 22, 23, 24, 28, 29, 30, 31, 34, 37, 38, 39, 41, 45, 46, 47, \\
&52, 53, 54, 55, 56, 60, 61, 62, 63, 65, 69, 70, 71, 77, 78, 79, 80, 84, 85, 86, 87, \\
&88, 92, 93, 94, 95, 96, 101, 102, 103, 109, 110, 111, 112, 116, 117, 118, 119, 120, \\
&124, 125, 126 \ldots\}
\end{aligned}$$ [10]

Thus, nearly 800 years later, Emperor Ferdinand's request of Fibonacci has gone far, revealing deep and fascinating truths about the connection between rational numbers, squares, and integers. How much further will this quest go? There is no end, only deeper universes of beauty to be discovered. Perhaps this was what inspired the mathematician Charles Lutwidge Dodgeson, when he wrote, as Lewis Carroll, about how deep the rabbit hole goes.

References

[1] Keith Conrad, *The Congruent Number Problem.* Faculty Feature Article, University of Connecticut, 2007.

http://www.thehcmr.org/issue2_2/congruent_number.pdf

[2] V Chandrasekar, *The Congruent Number Problem.* Article in Resonance, August 1998.

http://www.ias.ac.in/resonance/Volumes/03/08/0033-0045.pdf

[3] Norbert Schappacher, *Diophantus of Alexandria : a Text and its History.* 2005.

[4] J.D. Sally and P.J. Sally Jr. *Roots to Research.* American Mathematical Society, Ch 2, p 97, 2007.

http://www-irma.u-strasbg.fr/∼schappa/NSch/Publications_files/Dioph.pdf

[5] Wikipedia, *Modularity Theorem*

http://en.wikipedia.org/wiki/Modularity_theorem

[6] Joseph H. Silverman *A Friendly Introduction to Number Theory*, 2nd ed. Prentice Hall, New Jersey, 2001.

[7] Sunil Chetty, *Congruent Numbers and Elliptic Curves.* College of Saint Benedict and Stain John's, 2011.

http://www.csbsju.edu/Documents/Math/Sunil-CSBSJU-2011-09-08.pdf

[8] Neal Koblitz, *Introduction to Elliptic Curves and Modular Forms.* Springer-Verlag, New York, 1984.

http://www.drchristiansalas.org.uk/MathsandPhysics/Modular/KoblitzModularForms.pdf

[9] Guy Henniart, *Congruent Numbers, Elliptic Curves, and Modular Forms.*

http://www.fen.bilkent.edu.tr/∼franz/publ/guy.pdf

[10] Online Encyclopedia of Integer Sequences, *The Congruent Numbers.* N.J.A. Sloane, 1964.

http://oeis.org/A003273