# The Congruent Number Problem and Connections to Elliptic Curves

MATH 605C Final Course Project

Luke Askew

Spring 2021

## 1 Introduction

There have been several proposed characterizations of congruent numbers in the millennia since their first introduction. Arab manuscripts from before 972CE appear to be the first known instance of the congruent number problem: provided an integer $k$, the problem is to find another integer $n$ such that $k$, $n^2 - k$ and $n^2 + k$ are all square numbers.[1]

Now if $x^2 + y^2 = z^2$, then $z^2 - 2xy = (x - y)^2$ and $z^2 + 2xy = (x + y)^2$, so we can find congruent integers by identifying areas of right triangles, letting $n := 2xy$, $n^2 \pm k := (x \pm y)^2$. Extending this definition to rational numbers, we have the following modern definition for congruent numbers:

**Definition 1.** *A rational number $r \in \mathbb{Q}$ is a* ***congruent number*** *if it is the area of a right triangle with rational sidelengths.*

By the pythagorian theorem and its converse, the condition of being a right triangle is equivalent to the condition $a^2 + b^2 = c^2$ and that $r$ is the area of this triangle is equivalent to the area formula for right triangles, $r = ab/2$. This provides a way of defining congruent numbers by the conditions of satisfying polynomial equations.

**Definition 2.** *A rational number $r \in \mathbb{Q}$ is a* ***congruent number*** *if there exist rational numbers $a, b, c$ such that $a^2 + b^2 = c^2$ and $r = ab/2$*

For an example, take a favorite Pythagorean triple, say $5, 12, 13$ and find the area $= \frac{1}{2}5(12) = 30$, so 30 is a congruent number. Notice if we rationally scale all sidelengths of this triangle this triangle by $s$, we have that $\frac{1}{2}s^2 5(12) = 30s^2$ is another congruent number. Generalizing this property allows for a more algebraic description of congruent numbers.

Let $\mathbb{Q}^+$ be the group of strictly positive rational numbers under multiplication. As seen from the previous example, since every congruent number will admit any rational square times it to also be a congruent number, the congruence property of $r \in \mathbb{Q}^+$ is determined uniquely by its coset in $\mathbb{Q}^+/(\mathbb{Q}^+)^2$. Each element of which will have as representative a squarefree rational number, and a unique least integer representation.[2, 3]

To find the unique integer representation for a coset represented by $\frac{a}{b}$, we take the prime factorization of $a$ and $b$ and remove any even multiples of a prime factor by multiplying by a fraction with that prime power squared, leaving each prime showing up once in the numerator or denominator. Multiplying by each element of the denominator squared produces the integer representation. For example $\frac{27}{245} = \frac{3^3}{(5)7^2} \equiv \frac{7^2}{3^2}\frac{3^3}{(5)7^2} = \frac{3}{5} \equiv 15$, and we will later confirm that 15 is a congruent number.

**Lemma 1.** *Suppose $r \in \mathbb{Q}^+/(\mathbb{Q}^+)^2$ has the congruence property, then there exists a Pythagorean triple $x, y, z$ such that $r = \frac{1}{2}xy$.*

As $r$ is a congruent number, there exists $n$ such that $r \pm n$ are square numbers. Use this to create the correspondence $r \to (\sqrt{r+n} - \sqrt{r-n}, \sqrt{r+n} + \sqrt{r-n}, 2\sqrt{r})$ which satisfies $a^2 + b^2 = c^2$.

Assuming the well known formula for computing all primitive Pythagorean triples from a tuple of integers, provided a tuple $(n, m)$ with $n < m$, all Pythagorean triples are found with $a = m^2 - n^2, b = 2mn, c = n^2 + m^2$. Since we arrive at all primitive Pythagorean triples through running this computation over all such tuples, every coset satisfying the congruence property is identified, eventually. Consider the following implementation:

```
triples = []
for m in range(2,10):
    for n in range(1,m):
        triples.append([m^2 - n^2 , 2*m*n, n^2 + m^2])
triples
```

We get the following results:

| a | b | c | r | coset representative |
|---|---|---|---|---|
| 3 | 4 | 5 | 6 | 6 |
| 8 | 6 | 10 | 24 | 6 |
| 5 | 12 | 13 | 30 | 30 |
| 15 | 8 | 17 | 60 | 15 |
| 12 | 16 | 20 | 96 | 6 |
| 7 | 24 | 25 | 84 | 21 |
| 24 | 10 | 26 | 120 | 30 |
| 21 | 20 | 29 | 210 | 210 |
| 16 | 30 | 34 | 240 | 15 |
| 9 | 40 | 41 | 180 | 5 |
| | | ... | | |
| 13 | 84 | 85 | 546 | 546 |
| 63 | 16 | 65 | 504 | 14 |
| 60 | 32 | 68 | 960 | 15 |
| 55 | 48 | 73 | 1320 | 330 |
| 48 | 64 | 80 | 1536 | 6 |
| 39 | 80 | 89 | 1560 | 390 |
| 28 | 96 | 100 | 1344 | 21 |
| 15 | 112 | 113 | 840 | 210 |

This output demonstrates some deficiencies of the algorithm. The representatives $6, 30, 15$, and 210 have already shown up in the list multiple times, so while this algorithm will provide all cosets with the congruent number property eventually, any given coset might take a very long time to be verified. Most importantly, while this algorithm allows for finding all congruent numbers, it does not offer proof that any number is not congruent.

The first result in this vein was that 1 is not a congruent number. Fermat invented the method of descent to prove this, showing that if there is one solution for a right angled triangle with integral sides with square area, then there exists another triangle with integer square area and integer sides with a smaller hypotenuse which provides a contradiction, however generalizing such a proof for more congruent numbers is difficult. Using more recent results with elliptic curves allows us to find methods for showing many other numbers are not congruent. [1]

## 2 Elliptic Curves of the Form $y^2 = x^3 - n^2x$

For congruent numbers $n$, the pythagorian triples making $n$ congruent are associated with the group of rational points on a related elliptic curve. In this section, we give an overview of this connection and consider the family of elliptic curves it provides.

**Theorem 1.** *There is a bijection between the sets* $\{(a, b, c)|a^2+b^2 = c^2, ab/2 = n\}$ *and* $E(\mathbb{Q})\backslash\{(n, 0), (-n, 0), (0, 0), \infty\}$ *for* $E = y^2 = x^3 - n^2x$.

Two inverse correspondences are given by $\psi(a, b, c) = (\frac{nb}{c-a}, \frac{2n^2}{c-a})$ and $\varphi(x, y) = (\frac{x^2-n^2}{y}, \frac{2nx}{y}, \frac{x^2+n^2}{y})$.

These formulas explain the points we exclude from $E(\mathbb{Q})$. Under the correspondence, producing $\varphi(\pm n, 0)$ requires division by 0 and the point at infinity corresponds to a degenerate triangle with $a^2 = c^2$.

We only show the composition $\varphi \circ \psi$ is the identity, referring the interested reader to [1].

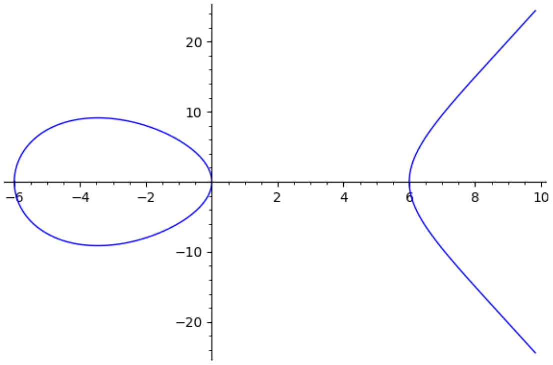
$$\begin{aligned}
\varphi(\psi(a, b, c)) &= \varphi((\frac{nb}{c-a}, \frac{2n^2}{c-a})) \\
&= (\frac{{\frac{nb}{c-a}}^2 - n^2}{\frac{2n^2}{c-a}}, \frac{2n\frac{nb}{c-a}}{\frac{2n^2}{c-a}}, \frac{{\frac{nb}{c-a}}^2 + n^2}{\frac{2n^2}{c-a}}) \\
&= (\frac{-2a^2 + 2ca}{2(c-a)}, b, \frac{2c^2 - 2ca}{2(c-a)}) \\
&= (a, b, c)
\end{aligned}$$

With this connection, we turn our attention to study elliptic curves of the form $y^2 = x^3 - n^2x$. Notice that if the rank of this curve is greater than zero, there are infinitely many corresponding Pythagorean triples, and so $n$ is a congruent number. Similarly, if $n$ is not a congruent number, the rank should be zero and any points of $E(\mathbb{Q})$ not the identity must have $y = 0$.

We note two important facts about these curves that will come in handy later: $E : y^2 = x^3 - n^2x$ has complex multiplication by the map $(x, y) \to (-x, iy)$ and for primes $p \cong 3 \mod 4$, there are $p + 1$ points of $E$ over $\mathbb{F}_p$. We see the second fact is true by the same argument used in class to count the points on

$F : y^2 = x^3 + x$ because $-(x^3 - n^2x) = (-x)^3 - n^2(-x)$, the group of squares has index 2 in the multiplicative group $(\mathbb{Z}/p\mathbb{Z})^*$, and $-1$ is not a square $\mod p$.

Since it is easy to see that 6 is a congruent number by the $3-4-5$ triangle, we take for example the elliptic curve $E : y^2 = x^3 - (6)^2x$, and after a Sage computation we find that the rank of this elliptic curve is 1, so there are infinitely many points on $E(\mathbb{Q})$ showing 6 to be a congruent number. We depict this elliptic curve below.



Again using Sage, we identify the point $(1442401/19600, 1726556399/2744000)$. This point is the first multiple of a generator for $\mathbb{Z}$ in $E(\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}$ such that all entries are positive. We then locate the corresponding triangle with sidelengths $(1437599/168140, 2017680/1437599, 2094350404801/241717895860)$ by the above formulas. Sure enough, this triangle has area 6. Using the inverse formula for the triple $(3, 4, 5)$, we find the point $(12, 36)$ which is the sum of the generator $(-3, 9)$ for $\mathbb{Z}$ with the torsion point $(0, 0)$.

## 2.1 Torsion

The previous example raises an important question: what is going on with the torsion subgroups for elliptic curves of the form $y^2 = x^3 - n^2x$? In the example, as $E(\mathbb{Q})_{tors} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, all elements of the torsion subgroup have order 2 and therefore have $y$ component equal to zero. This is an example of the following theorem:

**Theorem 2.** *For any $n$, $E : y^2 = x^3 - n^2x$ has $E(\mathbb{Q})_{tors} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.*

We will give a proof and a sketch of this theorem, each using a theorem beyond the scope of this paper. The proof uses the Nagell-Lutz theorem for a quick verification and the sketch will use more elementary tools along with Dirichlet's theorem.

Before we move on, because we know the projective points $(n, 0, 0), (-n, 0, 0), (0, 1, 0), (0, 0, 1)$ are the only elements of $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ that don't correspond to right triangles, we know that there points on $E$ corresponding to right triangles for $n$, i.e. $n$ is a congruent number, if and only if free part of $E(\mathbb{Q})$ contains a point that is nontrivial.

**Corollary 1.** *$n$ is a congruent number if and only if the rank of $E(\mathbb{Q})$ is greater than zero*

Notice further that the correspondence will also provide us that if a rational number is the area of a rational right triangle, then there are infinitely many rational right triangles with the same area. This also provides an alternative proof that 1 is not a congruent number as $y^2 = x^3 - (1)^2x$ has rank 0 by a Sage calculation. Similarly, we compute the rank of the first 41 curves of the form $y^2 = x^3 - n^2x$, finding that the first congruent numbers are $5, 6, 7, 13, 14, 20, 21, 22$ and so forth:

| | | | | | |
|---|---|---|---|---|---|
| n, rank | 7 , 1 | 14 , 1 | 21 , 1 | 28 , 1 | 35 , 0 |
| 1, 0 | 8 , 0 | 15 , 1 | 22 , 1 | 29 , 1 | 36 , 0 |
| 2 , 0 | 9 , 0 | 16 , 0 | 23 , 1 | 30 , 1 | 37 , 1 |
| 3 , 0 | 10 , 0 | 17 , 0 | 24 , 1 | 31 , 1 | 38 , 1 |
| 4 , 0 | 11 , 0 | 18 , 0 | 25 , 0 | 32 , 0 | 39 , 1 |
| 5 , 1 | 12 , 0 | 19 , 0 | 26 , 0 | 33 , 0 | 40 , 0 |
| 6 , 1 | 13 , 1 | 20 , 1 | 27 , 0 | 34 , 2 | 41 , 2 |

With the utility of this theorem assured, we turn our attention to its first proof requiring a theorem of Nagell and Lutz.

**Theorem 3.** *Let $E$ be an elliptic curve over $\mathbb{Q}$ with Weierstrass equation $y^2 = x^3 + Ax + B$ with $A, B \in \mathbb{Z}$, then if $P \in E(\mathbb{Q})$ is a nonzero torsion point then the $x$ and $y$ coordinates of $P$, $x(P), y(P) \in \mathbb{Z}$ and either $P$ is a 2-torsion point or else $y(P)^2$ divides $4A^3 + 27B^2$.*

[3, 240]

Using this result we verify our torsion theorem.

*Proof.* In the case of $E : y^2 = x^3 - n^2x$, $A = -n^2$ and $B = 0$, so if a torsion point $P$ is not 2-torsion, $y(P)^2 | 4n^6$ hence $y(P)|2n^3$ and $y(P) = 2kn^3$ for some $k \in \mathbb{Z}$. Solving for $x(P)$, requires solving $x(P)^3 - n^2x(P) - 4k^2n^6 = 0$. Applying the cubic formula, two solutions over $\mathbb{C}$ are imaginary and the only real solution is irrational, so $P \notin E(\mathbb{Q})$. □

For the second proof, we will require Dirichlet's theorem on primes in arithmetic progression to derive a contradiction.

**Theorem 4** (Dirichlet's theorem)**.** *If $q$ and $l$ are relatively prime positive integers, then there are infinitely many primes of the form $l + kq$ with $k \in \mathbb{Z}$*

We can now give an alternate argument for theorem 2 following a similar proof given in [2, 44].

**Sketch 1.** *First, consider $E$ as a curve in $\mathbb{P}^2_{\mathbb{Q}}$. Each point in $\mathbb{P}^2_{\mathbb{Q}}$ can be represented as a triple of integers with no common factor, so we can define a map $\varphi_p : \mathbb{P}^2_{\mathbb{Q}} \to \mathbb{P}^2_{\mathbb{F}_p}$ by reduction modulo $p$ for all primes $p$. Now $\varphi_p$ restricted to $E(\mathbb{Q})$ maps to $E(\mathbb{F}_p)$ since $y^2z = x^3 - n^2xz^2$ satisfied for any integer triples $(x, y, z)$ is also satisfied modulo $p$, and as the result of adding two points on $E(\mathbb{Q})$ and reducing modulo $p$ is the same as reducing modulo $p$ and adding the points on $E(\mathbb{F}_p)$, therefore $\varphi$ is a group homomorphism.*

*By a messy congruence calculation, we have that for $P, Q \in E(\mathbb{Q}), \varphi_p(P) = \varphi_p(Q)$ if and only if $p$ divides each component in the cross product $P \times Q$ considered as vectors in $\mathbb{Q}^3$.*

*Now for a contradiction we assume $E(\mathbb{Q})_{tors} \not\cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Then there are at least three and at most $\binom{|E(\mathbb{Q})_{tors}|}{2}$ pairs of points $x, y \in E(\mathbb{Q})_{tors}$ with no two colinear. We see this means that taking the list of all components in the cross products over all pairs $x, y$, we will find a greatest component, so by the previous paragraph $\varphi_p(x) = \varphi_p(y)$ only if $x = y$ for all primes $p$ greater than the greatest component, thus $\varphi_p$ is injective for all $p >> 0$.*

*Let $\ell > 2$ be the order of an element the finite group $E(\mathbb{Q})_{tors}$ which exists by the contradiction hypothesis. Now as $\mathbb{Z}/\ell\mathbb{Z} \leq E(\mathbb{Q})_{tors}$ is a subgroup and $\varphi$ is injective for all $p >> 0$, $\mathbb{Z}/\ell\mathbb{Z} \leq E(\mathbb{F}_p)$. By Lagrange's theorem, $\ell$ divides $|E(\mathbb{F}_p)| = p + 1$ for all but finitely many $p \equiv 3 \mod 4$, so for these $p$ we have $p \equiv -1$*

mod $\ell$. *Now for each possible $\ell$, we can find a relatively prime integer $t \equiv 3 \mod 4$ so that there are only finitely many $\ell k + t$ prime contradicting Dirichlet's theorem. For example, if $\ell = 8$, this implies there are finitely many primes of the form $8k + 3$ since $8k + 3 \equiv 3 \not\equiv -1 \mod \ell$.*

## 2.2 Rank

In the previous section, we computed the ranks of the first 41 elliptic curves of the form $y^2 = x^3 - n^2x$, with the lowest rank being 0 and the highest being 2. In this section, we consider different restrictions on the rank of these elliptic curves. Throughout this section $E$ and $n$ will be defined by $E : y^2 = x^3 - n^2x$.
Let $\mathcal{P}$ denote the set of all integer primes and $\infty$, and $V_p : \mathbb{Q} \to \mathbb{Z}$ be defined for $a/b \in \mathbb{Q}$ to be the multiplicity of $p$ as a factor of $a$ minus the multiplicity of $p$ as a power of $b$. For example, take $a/b = 15/12 = (3(5))/(2^2(3))$, then $v_2(15/12) = 0 - 2 = -2, v_3(15/12) = 1 - 1 = 0$, and $v_7(15/12) = 0$.

We define the set $\mathbb{Q}(S, 2) = \{a \in \mathbb{Q}/(\mathbb{Q})^2 | v_p(a) \not\equiv 0 \mod 2, \forall p \in \mathcal{P} \setminus S\}$ which fancy notation to take all equivalence classes in $\mathbb{Q}/(\mathbb{Q})^2$ with unique minimal integer representation a combination of the elements of $S$. Notice that $\mathbb{Q}(S, 2)$ defines an Abelian group under multiplication isomorphic to $(\mathbb{Z}/2\mathbb{Z})^{\times k}$ for some $k \in \mathbb{Z}$ as each prime in $S$ can show up 0 or 1 in the minimal integer representation, and multiplication of least integer representations both possessing the same prime results in an even, hence vanishing multiplicity in the product.

**Theorem 5.** *There exists an injective group homomorphism $b : E(\mathbb{Q})/2E(\mathbb{Q}) \to \mathbb{Q}(S, 2) \times \mathbb{Q}(S, 2)$.*

This injection is given by

$$b(P) = \begin{cases} (1,1) & P = (\infty) \\ (-1,-n) & P = (0,0) \\ (n,2) & P = (n,0) \\ (x, x-n) & P = (x,y) \neq (\infty), (0,0), (n,0) \end{cases} \qquad [4]$$

Verifying a case for $n = 6$, we have that $S = \{2, 3, \infty\}$ and $\mathbb{Q}(S, 2) = \{\pm1, \pm2, \pm3, \pm6\}$. Let's take the elements $(-3, -9)_E$ and $(6, 0)_E \in E(\mathbb{Q})/2E(\mathbb{Q})$ which add to $(-2, 8)_E$ using the addition law from $E$.

$b((-3, -9)_E) = (-3, -9)_S \equiv (-3, 1)_S \in \mathbb{Q}(S, 2)\times\mathbb{Q}(S, 2)$. Furthermore, $b((6, 0)_E) = (6, 2)_S$ and $b((-2, 8)_E) = (-2, -8)_S \equiv (-2, -2)_S$.

Now taking the addition in $\mathbb{Q}(S, 2) \times \mathbb{Q}(S, 2)$, we have that $(-3, 1)_S + (6, -2)_S = (-18, -2)_S \equiv (-2, -2)_S$, so we have that

$$b((-3, -9)_E) + b((6, 0)_E) = b((-3, -9)_E + (6, 0)_E)$$

.

Studying the domain on this injection, we consider $E(\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}^r$. This has $2\mathbb{Q} \cong \mathbb{Z}^r$, thus $E(\mathbb{Q})/2E(\mathbb{Q}) \cong (\mathbb{Z}/2\mathbb{Z})^{r+2}$ . Solving for $r$, we have that

$$r = \log_2(\frac{|im(b)|}{4}).[4]$$

Now provided an integer $n$ and its unique minimal representative $n' \in \mathbb{Q}/(\mathbb{Q})^2$, we have that $n' = 2^\delta p_1 p_2 ... p_\ell$ where $\delta \in \{0, 1\}$, so the cardinality of $\mathbb{Q}(S, 2)$ is $2^{\ell+2}$. As the size of the image is bounded by the size of $\mathbb{Q}(S, 2) \times \mathbb{Q}(S, 2)$, $|im(b)| \leq 2^{2\ell} + 4$.

$$r \leq \log_2(\frac{2^{2\ell+4}}{4}) = 2 + 2\ell.$$

We can do better if we begin to consider how large $im(b)$ is within $\mathbb{Q}(S, 2) \times \mathbb{Q}(S, 2)$.

**Theorem 6.** *Suppose $b(P) = (x_1, x_2) \neq (\infty, \infty), (0, 0), (n, 0)$, then there exist $z_1, z_2 \in \mathbb{Q}^*, z_3 \in \mathbb{Q}$ such that $x_1z_1^2 - x_2z_2^2 = n$ and $x_1z_1^2 - x_1x_2z_3^2 = -n$, and in this case $P = (x_1z_1^2, x_1x_2z_1z_2z_3) = (x_2z_2^2 + n, x_1x_2z_1z_2z_3)$.*

In [4], Serf provides a page of unsolvability conditions derived from this result, but we consider only the first: $x_1x_2 < 0$. Using this condition, we see we can half the possibilities for elements coming from the fourth piecewise definition from our previous bound.

$$r \leq \lfloor \log_2(\frac{2^{2\ell+4} - (\frac{2^{2\ell+4}-3}{2})}{4})\rfloor = \lfloor log_2(2^{2\ell}(4 - 2 + \frac{3}{2^{\ell+3}}))\rfloor = \lfloor 2\ell log_2(2 + \frac{3}{2^{\ell+3}})\rfloor = 2\ell.$$

The last equality comes $2xlog_2(2 + \frac{3}{2^{x+3}}) - 2x < 1$ for all $x > 0$. We have to be careful when $\ell$ is even to only subtract $\frac{2^{2\ell+4}-2}{2}$for parity, but this provides the same bound as the intuitive calculation above that works for $\ell$ odd.

This states that if $E : y^2 = x^3 - p^2x$ for $p$ a square multiple of a prime, the rank of $E$ is less than or equal to 2. We have already seen an example with $p = 41$ of this rank being achieved for an elliptic curve, so this bound is great for $\ell$ small, however the other conditions will help for $\ell$ large. Take (3)(7)(17)(97)(313) for example - we find that the rank is less than or equal to 10 while in [4] other conditions on $z_1, z_2$, and $z_3$ can bring this bound down to 4. Further showing our bound is best used for $\ell$ small, as 2 is not congruent, our bound works for $\ell = 0$ too!

A question we might ask is whether this bound limits the rank of all elliptic curves of our considered form. The following theorem dashes these hopes:

**Theorem 7.** *There are congruent numbers with arbitrarily many odd prime factors.*

*Proof.* Let $d = p_1...p_\ell$ with each $p_i$ distinct and odd, then we show there is a congruent number with at least $\ell$ prime factors with multiplicity 1. Notice that $2d, d^2 - 1$, and $d^2 + 1$ constitute a pythagorian triple as

$$(d^2 - 1)^2 + (2d^2) = d^4 - 2d^2 + 1 - 4d^2 = (d^2 + 1)^2.$$

This provides that $2d(d^2 - 1)$ is a congruent number. Now $p_i|d$, $p_i|d^2$, hence $d^2 - 1 \mod_{p_i} \equiv p_i - 1 \neq 0$, so $2d(d^2 - 1)$ is a congruent number divisible by each $p_i$ exactly once. □

Finally, the the largest rank we know of for a curve of the form $y^2 = x^3 - n^2x$ is 6. Klopf found at least 61 values of $n$ providing this rank, the smallest of which being $n = 6,611,719,886$. [5] Related to our previous inquiry, $6,611,719,886 = (2)(23)(143733041)$ has 3 prime factors, so our bound $r \leq 2\ell$ is sharp for $\ell = 3$.

# 3 Tunnell's Theorem

## 3.1 $L$ functions, Analytic Rank, and the Birch and Swinnerton-Dyer Cojecture

Tunnell's theorem uses analytic methods to determine if a given integer is congruent. We begin by developing the basic definitions that allow for understanding the statement of this correspondence.

Recall that $\#E/\mathbb{F}_p = p + 1 - a_p$ where $|a_p| \leq 2\sqrt{p}$ by the Hasse Weil bound, and the Hasse-Weil $L$-function is given by

$$Z_p(E, T) = \exp(\sum_{n=1}^{\infty} \frac{N_{p^n}}{n} T^n)$$

where $N_{p^n}$ counts the number of points of $E$ over $\mathbb{F}_{p^n}$.

We have from class

$$Z_p(E,T) = \frac{L(E,T)}{(1-T)(1-pT)}$$

where $L(E,T) = 1 - a_pT + pT^2$. Calculating, we see $Z_p(E,p^{-s}) = \frac{1}{1-a_pp^{-s}+pp^{-2s}}$.Using this characterization of the Hasse-Weil L-function we define the partial $L$ function of an elliptic curve.

**Definition 3.** *Let $\Delta$ be the discriminant of $E$. The partial $L$ function of $E$ is defined as*

$$L(\tilde{E},s) = \prod_{p\nmid\Delta} Z_p(E,p^{-s})$$

*where p is prime.*

$\tilde{L}(E,s)$ is messy to work with, and there are methods requiring a product over all primes to clean it up, similar to writing Euler's form for $\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_p \frac{1}{1-p^{-s}}$. We therefore make the following definition:

**Definition 4.** *The full L function of E is*

$$L(E,s) = \prod_{p\nmid\Delta} Z_p(E,p^{-s}) \prod_{p|\Delta} \frac{1}{1-a_pp^{-s}}$$

This product formula for the $L$-function of an elliptic curve is known to converge when $Re(s) > 3/2$, but in defining the analytic rank of an elliptic curve we desire to know the order of vanishing at $s = 1$.

Recall $\Gamma_0(N) = \{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) | c \equiv 0 \mod N\}$ and $Y_0(N) = \mathbb{H}/\Gamma_0(N)$ is the moduli space classifying ordered pairs $(E,E')$ of elliptic curves with a cyclic isogeny of degree (kernel of cardinality) $N$ between them. Equivelantly, for any $\tau \in \mathbb{H}$, its image in $Y_0(N)$ is the tuple $(F,G)$ where $F$ is the elliptic curve defined by $F : \mathbb{C}/(\mathbb{Z}+\tau\mathbb{Z})$ and $G$ is the cyclic subgroup generated by $1/N$. $X_0(N)$ is the compactification of $Y_0(N)$.[6]

**Definition 5.** *An elliptic curve $E$ is modular if it has a modular parameterization by $X_0(N)$. Equivalently, if there exists an analytic function $I_\varphi : X_0(N) \to \mathbb{C}/L \cong E$ defined by $\varphi(\tau)$ a modular form of weight 2 for $\Gamma_0(N)$ and $I_\varphi(\tau) = 2\pi i \int_{i\infty}^{\tau} \varphi(z)dz$.[6]*

It turns out that if an elliptic curve over $\mathbb{Q}$ is modular then it has an analytic continuation to $\mathbb{C}$. As all elliptic curves are modular over $\mathbb{Q}$, there exists the analytic continuation needed to define the analytic rank.[7]

**Definition 6.** *The analytic rank of $E$ is the order of vanishing of the analytic continuation of $L(E,s)$ at $s = 1$.*

The term analytic rank suggests that the analytic rank of $E$ has to do with the rank of $E(\mathbb{Q})$. The weak form of the Birch and Swinnerton-Dyer conjecture makes this suggestion explicit.

**Conjecture 1** (Birch and Swinnerton-Dyer)**.** *The analytic rank and algebraic rank of an elliptic curve are equal.*

## 3.2 Gross and Zagier's Theorem

Gross and Zagier provide a result making tremendous progress on the Birch and Swinnerton-Dyer conjecture for elliptic curves with complex multiplication.

**Theorem 8** (Gross and Zagier)**.** *Let $E$ have complex multiplication and assume that $L(E,1) = 0$. Then if $L'(E,1) \neq 0$, then $E(\mathbb{Q})$ contains elements of infinite order. Furthermore, the analytic rank and algebraic rank of an elliptic curve are equal.[8]*

Their theorem is stated in slightly more generality in the original paper, but this form follows as their theorem demonstrates the strong form of the Birch and Swinnerton-Dyer conjecture. It is beyond the ability of this author to fully reproduce the result, so we will consider a construction used in the proof. Heegner points have many characterizations, including purely algebraic definitions, but we describe only one of many analytic views here.

Heegner points correspond to elements of $Y_0(N)$ with both elements of the pair $(E, E')$ having complex multiplication by the same ring $\mathcal{O} = End(E) = End(E')$, or equivalently a point of $Y_0(N)$ corresponding to $(F, G)$ where $F$ and $F/G$ have the same discriminant. [6]

Finding Heegner points *on an elliptic curve* comes down to evaluating $I_\varphi(\tau)$ for $\tau \in Y_0(N)$ a Heegner point. The purpose of finding these points is that they will end up yielding a nontorsion point when handled with care. [6]

We can find Heegner points for an elliptic curve using Sage. Sage elliptic curve point objects have a method for determining their rational coordinates called by `P.point_exact()` taking as an argument a Heegner discriminant which Sage finds with `E.heegner_discriminants_list()`. The exact method failed for all Heegner discriminants for several tested curves, including curves of rank $0, 1$, and $2$, so we instead use `P.numerical_approx()`.

For the rank 1 curve $E : y^2 = x^3 - 14x$, we have the following session:

```
E = EllipticCurve([-14^2,0])
E.heegner_discriminants_list(10)
> [-31, -47, -55, -87, -103, -111, -143, -159, -167, -199]
P = E.heegner_point(-55)
P.numerical_approx(prec=53)
> (28.1626799231567 + 2.01561916378864e-13*I : 129.680242362636 + 1.69684231943190e-12*I : 1.00000000000000)
P = E.heegner_point(-55)
P.numerical_approx(prec=53)
> (-4.26408730345284 - 1.78500768190372*I : 28.6239081901139 + 4.50989433237413*I : 1.00000000000000)
```

When testing an elliptic curve with $n = 3$, a rank 0 curve, all the Heegner point approximations had imaginary component of at least 0.1, and there should not be Heegner points on the curve giving us a rational coordinate. We should have found rational coordinates with the Heegner point method for the curve in the above session, so this led us to believe that `28.1626799231567` 2.01561916378864e-13*I : 129.680242362636 + 1.69684231943190e-12*I : 1.00000000000000+ might correspond closely to a rational point on the curve. We implemented the following search:

```
for n in range(2):
    for l in range(2):
        for k in range(-30,100):
            item = (n*E.torsion_subgroup().gens()[1] + l*E.torsion_subgroup().gens()[0] + k*E.gens()[0])
            if item[0].n(17) < 28.17:
                if item[0].n(17) > 28.15:
                    print(n,k,l,item[0].n(17), item , "\n")
```

This resulted in us finding that $72(18 : 48 : 1) \approx (28.155 : 129.617 : 1)$, though the $x$-coordinate alone represented as a string has 9610 characters. While this might be the Heegner point we were looking for, increasing the precision of the Heegner point numerical approximation did not lead much closer to this conjectured rational value, but if this rational value is indeed a Heegner point, then we have found a point of infinite order as promised. In [6], Elkies considers related curves of the form $Ay^2 = x^3 - x$ which are a family which can also be related to the congruent number problem, finding rational solutions with an analytic method which inspired the one we attempted here.

Another result using Heeger points is that primes equivalent to 5 or 7 $\mod 8$ are congruent numbers.[9, 618] Using this along with our previous results on the ranks of elliptic curves of the form $y^2 = x^3 - n^2x$, we can find some elliptic curves with massive coefficients and know their rank is either 1 or 2. Take for example Mersenne primes which have $2^k - 1 \equiv 7 \mod 8$ for $k > 2$. $2^{82,589,933} - 1$ is known to be prime, so we know that the torsion of $y^2 = x^3 - (2^{82,589,933} - 1)^2x$ is either 1 or 2.

### 3.3 Tunnell's Partial Solution to the Congruent Number Problem

Tunnell provides a partial solution to the congruent number problem with the following theorem:

**Theorem 9.** *Let $g = q\prod_{n=1}^{\infty}(1-q^{8n})(1-q^{16n})$ and for $t \in \mathbb{N}$ $\theta_t = \sum_{n=-\infty}^{\infty} q^{tn^2}$ be formal power series in $q$. Define $a$ and $b$ by $g\theta_2 = \sum_{n=1}^{\infty} a(n)q^n$ and $g\theta_4 = \sum_{n=1}^{\infty} b(n)q^n$. Then for $n$ odd,*

- *if $a(n) \neq 0$ then $n$ is not a congruent number*
- *if $b(n) \neq 0$ then $2n$ is not a congruent number*

*[10]*

To prove this theorem, Tunnel considers modular forms of weight 3/2 to show the existence and uniqueness of $g$ can be reduced to a problem in Galois theory. Using $g$, he provides formulas for $a(n)$ and $b(n)$ in terms as Dirichlet series, for example showing $a(n) = \sum_{m=-\infty}^{\infty} c(n-2m^2)$, before calculating the equivelance of these formulas with the number of triples of integers integers satisfying degree two equations. In particular,

$a(n) = |\{(x,y,z)|2x^2 + y^2 + 32z^2 = n\}| - \frac{1}{2}|\{(u,v,w)|2u^2 + v^2 + 8w^2 = n\}|$
and
$b(n) = |\{(x,y,z)|16x^2 + 4y^2 + 32z^2 = n\}| - \frac{1}{2}|\{(u,v,w)|16u^2 + 4v^2 + 128w^2 = n\}|$.

Tunnel also proves that if the Birch and Swinnerton-Dyer conjecture is true for elliptic curves of the form $y^2 = x^3 - n^2x$ then the converse to his theorem holds, strengthening the statement to

- if $a(n) \neq 0$ if and only if $n$ is not a congruent number
- if $b(n) \neq 0$ if and only if $2n$ is not a congruent number

As we know by Gross and Zagier that elliptic curves with complex multiplication satisfy the conjecture, so this converse is now known to hold.

We can now fish with dynamite, achieving Fermat's result by simply by noticing $a(1) = 2 - \frac{1}{2}2 = 1$ implies that 1 is not congruent.

## 4 *t*-congruent Number Problem for Heron Triangles

Having been so mean to the multiplicative identity, we conclude by considering a problem where 1 is 18-congruent. The $t$-congruent number problem changes the right angle condition for having a congruent number to the condition of being a Heron triangle, a triangle with rational sidelengths. Instead of having a right angled triangle, take a triangle with angle $\theta$, then by trigonometry we have the new conditions $a^2 = b^2 + c^2 - 2bc\cos(\theta)$ and $2n = bc\sin(\theta)$. Since we would like to continue our search for rational solutions, we use the rational perametrization for sine and cosine, $\sin(\theta) = \frac{2t}{t^2+1}$ and $\cos\theta = \frac{t^2-1}{t^2+1}$ to motivate a definition.

**Definition 7.** *An integer $n$ is $t$-congruent if there are positive rational numbers $a, b$, and $c$ such that*

$$a^2 = b^2 + c^2 - 2bc\frac{t^2-1}{t^2+1}$$

*and*

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

[9]
In [11], Long found an "algorithm to determine a one-parameter family of elliptic curves associated to a one-parameter family of K3 surfaces with generic Picard number 19 by a Shioda–Inose structure.". As a consequence of this algorithm, Long found several interesting constructive proofs related to the $t$-congruent number problem by considering a family of elliptic curves related to the problem with positive rank.

**Lemma 2.** *For fixed $t$, $n$ is a $t$-congruent if and only if $n/t$ and $t^2+1$ are rational squares or the elliptic curve $E : y^2 = x(x-n/t)(x+nt)$ has $p \in E(\mathbb{Q}) \setminus E(\mathbb{Q})[2]$.*

Notice that 1-congruent numbers are congruent numbers by the preceding definition. Furthermore, for $t = 1$, we have that $t^2+1 = 2$ is not a rational square so $y^2 = x(x-n/t)(x+nt) = x^3+(nt-n/t)x^2-n^2x = x^3-n^2x$ must have $p \in E(\mathbb{Q}) \setminus E(\mathbb{Q})[2]$, exactly the theorem we proved previously.

Supposing $n$ is a $t$-congruent number, one can consider the point $p = ((\frac{a}{2})^2, \frac{(b^2-c^2)a}{8})$. Sparing the reader the long computation, using both of $a^2 = b^2+c^2-2bc\frac{t^2-1}{t^2+1}$ and $2n = bc\frac{2t}{t^2+1}$ we show $p \in E(\mathbb{Q})$, and as $y(p) \neq 0$, $p \notin E(\mathbb{Q})[2]$. The other construction supposing $n/t$ and $t^2+1$ are rational squares lets us take $a = 2\sqrt{n/t}$ and $b = c = \sqrt{\frac{n(t^2+1)}{t}}$. [11]

**Theorem 10.** *Every integer $n$ is $t$ congruent for some $t \in \mathbb{Q}$.*

Taking a triangle with sides $n-1/2$, $\frac{n(n^2+n+5/4)}{(n+1/2)(n-1/2)}$, $\frac{5/2n^2+1/2n+1/8}{(n+1/2)(n-1/2)}$ provides a triangle with area $n$ for $n \neq 2$ [11]. For example, taking $n = 1$ we have a triangle with sidelengths $1/2, 13/3, 25/6$ has area 1. By a simple calculation we see this provides that 1 is an 18-congruent number.

# References

[1] K. Conrad. The congruent number problem. [Online]. Available: https://kconrad.math.uconn.edu/articles/congruentnumber.pdf

[2] N. Koblitz, *Introduction to Elliptic Curves and Modular Forms.* Springer-Verlag, 1984.

[3] J. H. Silverman, *The Arithmetic of Elliptic Curves.* Springer, 2016.

[4] P. Serf, "Congruent numbers and elliptic curves," *Computational Number Theory*, 1991.

[5] M. Klopf, "Congruent number elliptic curves of high rank," Master's thesis, Graz University of Technology, 2015.

[6] N. D. Elkies. Heegner point computations. [Online]. Available: https://www.wstein.org/people/elkies/papers/ants1.ps

[7] A. J. Wiles, "Modular elliptic curves and fermat's last theorem," *Annals of Mathematics*, no. 141, pp. 443–551, 1995.

[8] B. H. Gross and D. B. Zagier, "Heegner points and derivatives of l-series," *Inventiones mathematicae*, vol. 84, pp. 225–320, 1986.

[9] J. Top and N. Yui, "Congruent number problems and their variants," *Algorithmic Number Theory*, vol. 44, pp. 613–639, 2008.

[10] J. Tunnel, "A classical diophantine problem and modular forms of weight 3/2," *Inventiones mathematicae*, vol. 72, pp. 323–334, 1983.

[11] L. Long, "On shioda–inose structures of one-parameter families of k3 surfaces," *Journal of Number Theory*, vol. 109, no. 2, pp. 299–318, 2004.