The Congruent Number Problem

Drew Miller and Ryan Yick

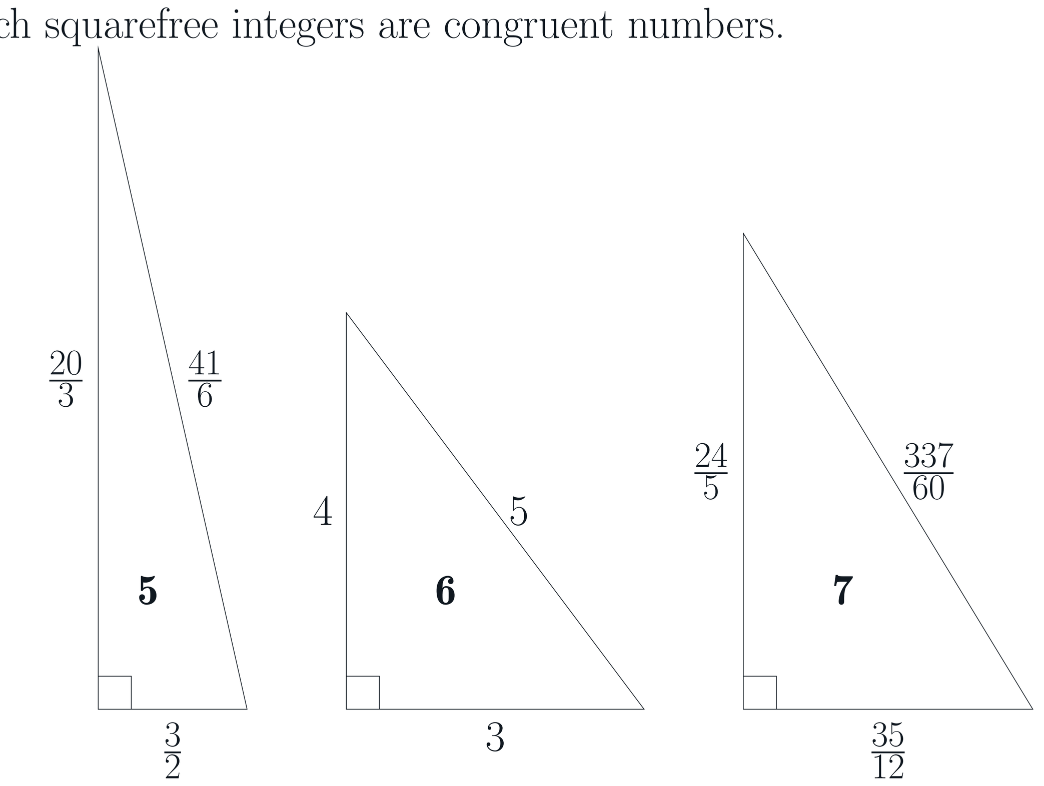
Department of Mathematics, University of California, Santa Barbara

Abstract

The congruent number problem is a classical problem in Diophantine geometry that asks questions on the area of rational right triangles. The conditions for a rational number n to be the area of a right triangle with rational side lengths was partially resolved by Tunnell in 1983. In this poster, we provide an overview of Tunnell's theorem as presented in [1] as well as an implementation of an algorithm to determine whether a number n is a so-called congruent number. Finally, we connect the theorem to the modern theory of elliptic curves.

Problem Formulation

A triangle is called **rational** if all of its sides are rational. A positive rational number n is called a **congruent number** if there exists a rational right triangle whose area is n. Equivalently, n is a congruent number if there are $a, b, c \in \mathbb{Q}_{>0}$ such that $a^2 + b^2 = c^2$ and $(1/2)ab = n$. The congruent number problem asks which positive rational numbers are congruent numbers. One can show that the question reduces to finding which squarefree integers are congruent numbers.



Pictured above are rational right triangles with areas 5, 6, and 7, respectively.

Tunnell's Theorem

A 1983 theorem of Jerrold Tunnell provides a partial resolution to the congruent number problem. If the famously unsolved Birch and Swinnerton-Dyer (BSD) conjecture is true for certain elliptic curves, Tunnell's theorem provides a complete resolution.

Theorem (Tunnell)**.** *Let n be a squarefree integer. Set*

$$\begin{aligned} f(n) &= \#\{(x,y,z) \in \mathbb{Z}^3 : x^2 + 2y^2 + 8z^2 = n\}, \\ g(n) &= \#\{(x,y,z) \in \mathbb{Z}^3 : x^2 + 2y^2 + 32z^2 = n\}, \\ h(n) &= \#\{(x,y,z) \in \mathbb{Z}^3 : x^2 + 2y^2 + 8z^2 = n/2\}, \\ k(n) &= \#\{(x,y,z) \in \mathbb{Z}^3 : x^2 + 2y^2 + 32z^2 = n/2\}. \end{aligned}$$

For odd n, if n is congruent, then $f(n) = 2g(n)$. For even n, if n is congruent, then $h(n) = 2k(n)$. Moreover, if the weak Birch and Swinnerton-Dyer conjecture is true for the curve $y^2 = x^3 - n^2x$, then the reverse implication is also true.

Tunnell's theorem provides a way to verify that a given n is not a congruent number: if $f(n) \neq 2g(n)$ (if n is odd) or $h(n) \neq 2k(n)$ (if n is even), then n cannot be a congruent number. We will provide an implementation of an algorithm that determines unconditionally if a given n is not congruent using Tunnell's theorem.

The Algorithm

Our algorithm shown below calculates Tunnell's Theorem by counting the number of solutions to the given equations given a certain number n, outputting whether n is not congruent or if the results are inconclusive. We were able to increase the efficiency of the algorithm by finding key observations that greatly limited the amount of numbers we need to check to find the number of solutions. Here were our observations:

1. Since x, y, and z are all squared, every term in the left-hand side of the equation will always be positive. This tells us two things:
   (a) Each term in the sum on the left has an upper bound:
      i. For $f(n)$ and $g(n)$, each term cannot exceed n;
      ii. For $h(n)$ and $k(n)$, each term cannot exceed $n/2$.
         A. In particular, for example in $k(n)$, for the term $32z^2$, we deduce that all solutions must have $-\sqrt{n}/8 \leq z \leq \sqrt{n}/8$.
   (b) For every solution that contains a positive x, y or z in the solution, there exists a similar solution with a negative x, y, or z. Thus we don't have to iterate through the possible negative solutions because they can all be accounted for through their positive counterparts.
2. Since the square of a number preserves its parity, x must always be odd.
   (a) For odd n, we use $f(n)$ and $g(n)$.
      i. For $f(n)$, for all $y, z \in \mathbb{Z}$, $2y^2 + 8z^2$ is even. Thus x must be odd in order for $x^2 + 2y^2 + 8z^2$ to be odd.
      ii. Similarly for $g(n)$, for all $y, z \in \mathbb{Z}$, $2y^2 + 32z^2$ is even so x must be odd.
   (b) For even n, we use $h(n)$ and $k(n)$.
      i. For all even squarefree integers n, $n/2$ is necessarily odd. If it were even, then $4 = 2^2 \mid n$ which implies that n was not squarefree.
      ii. Similar logic can be applied as above to show that x must be odd when considering $h(n)$ and $k(n)$.

Observation 1b) is incredibly useful, as it halves the amount of numbers we must iterate through to find solutions, however the only problem that arises is when x, y, and/or z equals 0. Since 0 is neither positive nor negative, then the number of 0's in a given solution affects the number of combinations of positive/negative solutions.

```
for x in range(1, int(math.sqrt(n) + 1), 2): #x has to be odd
    for y in range(0, int(math.sqrt(n/2) + 1)):
        for z in range(0, int(math.sqrt(n/8) + 1)):
            if (x**2 + 2*y**2 + 8*z**2 == n):
                count = count + 8  #8 different combinations of +-
                #solutions with 0 have less permutations
                if y == 0:
                    count = count - 4
                    if z == 0:
                        count = count - 2
                elif z == 0:
                    count = count - 4
return count
```

Since Tunnell's Theorem only works for n squarefree, we also added an `isSquareFree()` function which returns whether or not a given input is squarefree. It does this in a brute-force way by checking if any square integer divides the input. We also verified our code for Tunnell's theorem against the OEIS list of congruent numbers (sequence `A003273`) given in [2].

The Congruent Elliptic Curve $y^2 = x^3 - n^2x$

The converse of Tunnell's theorem holds on the assumption of the weak Birch and Swinnerton-Dyer conjecture for the elliptic curve $y^2 = x^3 - n^2x$. The BSD conjecture, one of the Millennium Prize problems, is an incredibly important conjecture in the field of arithmetic geometry, and even in mathematics as a whole. It relates elliptic curve data to the associated L-function. The details are not important for this poster.

This connection to Elliptic curves comes from [3], in which Tunnell proves his theorem using the classical Jacobi theta function

$$g = q\prod_{n=1}^{\infty}(1 - q^{8n})(1 - q^{16n})$$

as well as the classical theta functions

$$\theta_2 = \sum_{n\in\mathbb{Z}} q^{2n^2} \quad \text{and} \quad \theta_3 = \sum_{n\in\mathbb{Z}} q^{4n^2}.$$

Relating these to known results about L-functions and elliptic curves, Tunnell found this characterization of congruent numbers.

In particular, the so-called congruent elliptic curve $y^2 = x^3 - n^2x$ is relevant because there is a bijection between rational right triangles (a, b, c) with area n and rational points (x, y) on the elliptic curve $y^2 = x^3 - n^2x$ given by the correspondence

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

It is easy to show that this is indeed a bijection (i.e., the given maps are inverses). This correspondence shows that n is a rational number if and only $y^2 = x^3 - n^2x$ has nontrivial rational points. Thus we can use any tools for finding rational points on elliptic curves to identify congruent numbers.

Remarks

The congruent number problem, intimately related with the Birch and Swinnerton-Dyer conjecture, is nearly fully resolved, and indeed fully resolved provided the weak BSD is true for $y^2 = x^3 - n^2x$. Besides Tunnell's theorem, another known partial classification of congruent numbers is that for any prime p, if $p \equiv 3 \pmod 8$ then $2p$ is congruent, if $p \equiv 5 \pmod 8$ then p is congruent, and if $p \equiv 7 \pmod 8$ then both p and $2p$ are congruent.

Acknowledgements

We would like to thank the organizers of the 2021 UCSB Directed Reading Program for giving us an opportunity to learn about number theory. We also thank our mentor David Nguyen for his support, direction, and mentorship throughout the year.

References

[1] K. Conrad. *The Congruent Number Problem.* URL: https://kconrad.math.uconn.edu/blurbs/ugradnumthy/congnumber.pdf.

[2] N. Sloan. *The Online Encyclopedia of Integer Sequences.* URL: https://oeis.org/A003273.

[3] J. Tunnell. "A Classical Diophantine Problem and Modular Forms of Weight 3/2". In: *Invent. Math.* **72** (June 1983), pp. 323–334.